PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 03 May 2001 (03.05.01)	
International application No. PCT/JP00/05833	**Applicant's or agent's file reference** 900393
International filing date (day/month/year) 29 August 2000 (29.08.00)	**Priority date** (day/month/year) 30 August 1999 (30.08.99)
Applicant HATANAKA, Masayuki et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

09 March 2001 (09.03.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Kiwa Mpay
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Copy for the Elected Office (EO/US) PCT/JP00/05833

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

FUKAMI, Hisao
Mitsui Sumitomo Bank Minamimori-machi Bldg.
1-29, Minamimori-machi 2-chome
Kita-ku
Osaka-shi
Osaka 530-0054
JAPON

Date of mailing (day/month/year)
19 septembre 2001 (19.09.01)

Applicant's or agent's file reference
900393

IMPORTANT NOTIFICATION

International application No.
PCT/JP00/05833

International filing date (day/month/year)
29 août 2000 (29.08.00)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address

1) FUKAMI, Hisao 2) MORITA, Toshio
3) HORII, Yutaka
Sumitomo Bank Minamimori-machi Bldg.
1-29, Minamimori-machi 2-chome,
Kita-ku
Osaka-shi, Osaka 530-0054
Japan

State of Nationality:
State of Residence:
Telephone No.:
Facsimile No.:
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address

1) FUKAMI, Hisao 2) MORITA, Toshio
3) HORII, Yutaka
Mitsui Sumitomo Bank
Minamimori-machi Bldg.
1-29, Minamimori-machi 2-chome
Kita-ku
Osaka-shi
Osaka 530-0054
Japan

State of Nationality:
State of Residence:
Telephone No.:
Facsimile No.:
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

Authorized officer
Susumu KUBO
Telephone No.: (41-22) 338.83.38

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/05833

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F 17/60, G06K 19/00, G06K 19/10,
H04H 1/00, H04L 9/32,
H04M 3/42, H04M 3/493, H04M 11/08
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F 17/60, G06K 17/00, G06K 19/00-19/10,
H04H 1/00, H04L 9/32,
H04M 3/42, H04M 3/493, H04M 11/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shian Koho 1994-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 10-269144, A (Sony Corporation), 09 October, 1998 (09.10.98), Full text; all drawings (Family: none)	1-10,13-18
A	JP, 10-283268, A (Toshiba Corporation), 23 October, 1998 (23.10.98), Full text; all drawings (Family: none)	1-10,13-18
A	JP, 5-197635, A (Fujitsu Limited), 06 August, 1993 (06.08.93), Full text; all drawings (Family: none) 11-259964 (Sony Corporation)	1-10,13-18
P,A	JP, 11-283268, A (Toshiba Corporation), 24 September, 1999 (24.09.99), Full text; all drawings (Family: none)	1-10,13-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 December, 2000 (19.12.00)	26 December, 2000 (26.12.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/05833

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 11-12
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

In claims 11, 12, there is an expression "the first and second sets of maintenance information". However in claims 4,1 which claims 11, 12 refer to, there is only an expression "the first set of maintenance information", and there is no expression "the second set of maintenance information". Therefore claims 11, 12 are unclear.

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest

)特許協力条約に基づいて公開された国際

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年3 月8 日 (08.03.2001)

PCT

(10) 国際公開番号
WO 01/16820 A1

(51) 国際特許分類[7]: G06F 17/60, G06K 19/00, 19/10, H04H 1/00, H04L 9/32, H04M 3/42, 3/493, 11/08

(21) 国際出願番号: PCT/JP00/05833

(22) 国際出願日: 2000 年8 月29 日 (29.08.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願平11/243741 1999 年8 月30 日 (30.08.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP). 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP).

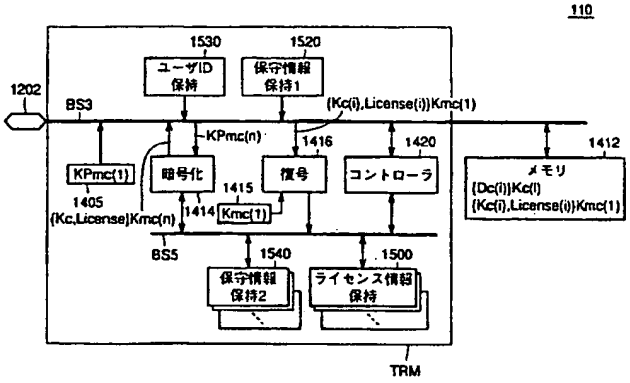
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 畑中正行 (HATANAKA, Masayuki) [JP/JP]. 蒲田 順 (KAMADA, Jun) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]. 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 小谷誠剛 (KOTANI, Seigou) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 利根川忠明 (TONEGAWA, Tadaaki) [JP/JP]; 〒187-8588 東京都小平市上水本町五丁目20番1号 株式会社 日立製作所 半導体グループ内 Tokyo (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI,

[続葉有]

(54) Title: RECORDING DEVICE

(54) 発明の名称: 記録装置



1530...HOLDING OF USER ID
1520...HOLDING 1 OF MAINTENANCE INFORMATION
1414...ENCRYPTING
1416...DECODING
1420...CONTROLLER
1412...MEMORY {Dc(i)}Kc(i){Kc(i),License(i)}Kmc(1)
1540...HOLDING 2 OF MAINTENANCE INFORMATION
1500...HOLDING OF LICENSE INFORMATION

(57) Abstract: A memory card (110) has a user ID holding part (1530) for holding user ID data for identifying the user of a memory card, a first maintenance information holding part (1520) for holding a first set of maintenance information for limiting the access to the memory card (110), and a second maintenance information holding part (1540) for holding a second set of maintenance information for limiting the access to each of groups of contents data. The memory card (110) identifies the user of the reproducing device on the basis of the user ID data and inhibits a person other than the authorized user from changing the first and second sets of maintenance information.

[続葉有]

WO 01/16820 A1

Miwa) [JP/JP]. 堀　吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).

(74) 代理人: 深見久郎, 外(FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

メモリカード（１１０）は、メモリカードのユーザを識別するユーザＩＤデータを保持するユーザＩＤ保持部（１５３０）と、メモリカード（１１０）に対するアクセスを制限する第１の保守情報を保持する第１の保守情報保持部（１５２０）と、コンテンツデータごとのアクセスを制限する第２の保守情報を保持する第２の保守情報保持部（１５４０）とを備える。メモリカード（１１０）は、ユーザＩＤデータに基づいて、再生装置側のユーザを識別し、正規なユーザ以外が第１および第２の保守情報を変更することを禁じる。

明細書

記録装置

技術分野

本発明は、携帯電話機等の端末に対して暗号化して配信された情報を格納して保持するための、メモリカードのなどの記録媒体として機能する記録装置の構成に関するものである。

背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物情報の配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作物情報の配信が行なわれた場合、各ユーザは、このようにして配信されたコンテンツデータを何らかの記録媒体に記録して保持することになる。

このような記録媒体としては、たとえばメモリカードのように電気的にデータの書込および消去が可能な媒体が用いられることになる。

この場合、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できるものとすると、著作権者の権利保護が図れない。

それのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なったり、コンテンツデータの移動や消去を自由に行なえることとすると、ユーザ側の権利保護にも支障を来たすことになる。

発明の開示

この発明の他の目的は、音楽データ等の著作物データを格納した記録媒体に保持されたコンテンツデータに対して、ユーザ以外の者が無断で再生、移転消去等を行なうことから保護する機能を備えたデータの記録媒体として機能する記録装置を提供することである。

係る目的を達成するために本願発明に係る記録装置は、暗号化コンテンツデータを再生出力する再生装置に対して着脱可能であって、暗号化コンテンツデータを受けて記録するための記録装置であって、データ入出力部と、第１の記憶部と、ユーザ情報保持部と、保護情報保持部と、制御部とを備える。

データ入出力部は、外部との間でデータの授受を可能とする。第１の記憶部は、データ入出力部からの暗号化コンテンツデータを格納する。ユーザ情報保持部は、記録装置のユーザを識別するための第１のユーザ特定データを保持する。保護情報保持部は、外部から与えられるユーザ情報と第１のユーザ特定データとの比較結果に応じて外部からの指示により更新可能な保護情報を保持する。

制御部は、記録装置の動作を制御する。制御部は、保護情報に基づいて、外部からの第１の記憶部に保持された暗号化コンテンツデータに対するアクセスを制限する。

好ましくは、制御部は、外部から与えられるユーザ情報と第１のユーザ特定データとが一致する場合に、ユーザ特定データの変更を可能とする。

本願発明にかかる配信システムでは、正規のユーザが受信してメモリ中に格納したコンテンツデータに対して、正規ユーザのみが再生、消去、移動処理を行な

うすることが可能な構成となっているので、正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

図面の簡単な説明

図１は、情報の配信を受けるための端末である携帯電話機１００の構成を説明するための概略ブロック図である。

図２は、図１に示したメモリカード１１０の構成を説明するための概略ブロック図である。

図３は、本発明の記録媒体が用いられる情報配信システムの全体構成を概略的に説明するための概念図である。

図４は、図３に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図５は、図３に示した音楽サーバ３０の構成を示す概略ブロック図である。

図６は、実施例１の情報配信システムにおけるコンテンツデータの配信動作を説明するためのフローチャートである。

図７は、メモリカード１１０に保持された暗号化コンテンツデータから、音楽情報を再生処理を説明するためのフローチャートである。

図８は、２つのメモリカード間において、コンテンツデータおよびキーデータとの移動を行なう処理を説明するための第１のフローチャートである。

図９は、２つのメモリカード間において、コンテンツデータおよびキーデータとの移動を行なう処理を説明するための第２のフローチャートである。

図１０は、本発明のメモリカード１１０の保守情報またはユーザＩＤデータＵｓｅｒ－ＩＤmの変更指示の処理を説明するためのフローチャートである。

図１１は、保守情報の考慮のある場合について、メモリカード１１０のコンテンツデータＤｃ（ｉ）の再生動作を説明するためのフローチャートである。

図１２は、メモリカード１１０中に保持されたコンテンツデータの消去動作を説明するためのフローチャートである。

図１３は、保守情報を考慮した場合において、移動処理を行なう場合の処理の流れを説明するためのフローチャートである。

図１４は、移動動作において受信側となっている場合、保守情報を考慮したときの追記処理を説明するためのフローチャートである。

図１５は、メモリカード１１０がコンテンツデータの配信を受ける状態を示す概念図である。

図１６は、２つのメモリカード１１０と１１２との間で、再生情報の移動が許可される場合を示す概念図である。

図１７は、２つのメモリカード１１０と１１２との間で、再生情報の移動が許可されない場合を示す概念図である。

図１８は、コンテンツデータ単位で、再生情報の転送を制御する場合の構成を示す概念図である。

図１９は、コンテンツデータ単位で、再生情報の転送を制御した場合に、ライセンス情報の移動が禁止されるときを示す概念図である。

発明を実施するための最良の形態

以下、本発明の実施例を図面とともに説明する。

［実施例１］

［配信データの受信端末（携帯電話）の構成］

図１は、本発明の記録媒体が使用される情報配信システムにおいて、情報の配信を受けるための端末である携帯電話機１００の構成を説明するための概略ブロック図である。

図１を参照して、携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機１００からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、携帯電話機１００の所有者を識別するためのユーザＩＤデータＵｓｅｒ－ＩＤｈを保持するユーザＩＤ保持部１１０７と、外部からの指示を携帯電話機１００に与えるためのタッチキー部１１０８と、コントローラ１１０６から出力される情報をユーザに視

覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバスＢＳ２に与え得る信号に変換し、または、データバスＢＳ２からのデータをコネクタ１１２０に与え得る信号に変換するための外部インターフェイス部１１２２とを備える。

ここで、たとえば、ユーザＩＤデータは、ユーザの携帯電話機の電話番号、またはユーザ自身が設定したデータ、あるいはその両者の組合せのデータ等を含む。

携帯電話機１００は、さらに、音楽サーバから供給される暗号化コンテンツデータを格納するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインターフェイス１２００と、メモリカード１１０からの暗号化されたコンテンツデータとこの暗号化されたコンテンツデータを復号するためのコンテンツキーＫｃとを受けて、音楽データを再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２と、デジタルアナログ変換部１５１２の出力を受けて、たとえば、ヘッドホーン（図示せず）と接続するための接続端子１５１４とを含む。

なお、説明の簡略化のため本発明の記録媒体中に格納された音楽データの配信および再生に係るブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、図１では一部割愛されている。

［メモリカードの構成］

図２は、図１に示したメモリカード１１０の構成を説明するための概略ブロック図である。

以下では、携帯電話機１００に装着されるメモリカード１１０に固有な秘密復号キーをキーＫｍｃ（１）とする。一方、他のメモリカードに固有な秘密復号キーをキーＫｍｃ（ｎ）（ｎ：自然数）とする。ここで、自然数ｎは、メモリカードを区別するためのものである。すなわち、キーＫｍｃ（ｎ）は、メモリカード

ごとに異なるものである。

また、これに対応して、秘密復号キーＫｍｃ（１）で復号可能な暗号化を提供し、キーＫｍｃ（１）とは非対称な、言い換えると同一の秘密復号キーＫｍｃ（１）に対して複数個存在し得る公開暗号化キーを公開暗号化キーＫＰｍｃ（１）と称し、同様にして、秘密復号キーＫｍｃ（ｎ）で復号可能な暗号化を提供し、キーＫｍｃ（ｎ）とは非対称な公開暗号化キーを公開暗号化キーＫＰｍｃ（ｎ）と称することとする。

図２を参照して、メモリカード１１０は、インターフェイス１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、公開暗号化キーＫＰｍｃ（１）を保持し、データバスＢＳ３に公開暗号化キーＫＰｍｃ（１）を出力するためのＫＰｍｃ（１）保持部１４０５と、端子１２０２およびデータバスＢＳ３を介して他のメモリカードから送信された公開暗号化キーＫＰｍｃ（ｎ）に基づいて、入力されたデータを暗号化するための暗号化処理部１４１４と、秘密復号キーＫｍｃ（１）を保持するためのＫｍｃ（１）保持部１４１５と、データバスＢＳ３から与えられるデータを受けて、Ｋｍｃ（１）保持部１４１５からの秘密復号キーＫｍｃ（１）に基づいて復号処理をするための復号処理部１４１６と、メモリカード１１０の動作を制御するためのコントローラ１４２０と、データバスＢＳ３を介して、配信される暗号化コンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）と、暗号化されたコンテンツキーおよびライセンス情報データ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）を格納し保持するためのメモリ１４１２とを含む。メモリ１４１２は、いわゆる半導体メモリであって、とくに限定されないが、たとえば、不揮発性メモリであるフラッシュメモリ等を用いることが可能である。

ここで、記号［Ｘ］Ｙは、復号キーＹで復号可能な暗号化処理でデータＸが暗号化されていることを表わす。

メモリカード１１０は、さらに、メモリカード１１０についてのユーザに関する情報であるユーザＩＤデータを保持するためのユーザＩＤ保持部１５３０と、メモリカード１１０に対する保守情報を保持するための第１の保守情報保持部１５２０と、復号処理部１４１６から出力される復号化されたデータを暗号化処理

部１４１４およびコントロール１４２０等へ伝達するためのデータバスＢＳ５と、コンテンツデータＤｃ（ｉ）に対応し、当該コンテンツデータの再生回数の制限等の再生権に関する情報やコンテンツデータの所有権等を示すライセンス情報データＬｉｃｅｎｓｅ（ｉ）を保持するためのライセンス情報保持部１５００と、コンテンツデータＤｃ（ｉ）（ｉ：自然数）ごとに設定されるコンテンツ保守情報を保持するための第２の保守情報保持部１５４０とを備える。

なお、上述した構成において、コンテンツデータＤｃ（ｉ）やコンテンツキーデータＫｃ（ｉ）、ライセンス情報データＬｉｃｅｎｓｅ（ｉ）等の自然数ｉは、各コンテンツデータごとにこれらのデータが異なることを表現している。

また、図２において実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。

このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）と呼ばれる。

もちろん、メモリ１４１２も含めて、モジュールＴＲＭに組込まれる構成としてもよい。しかしながら、図２に示したような構成とすることで、メモリ１４１２中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１２中のデータのみでは、音楽データ等のコンテンツデータを再生することは不可能である。このため、高価なタンパーレジスタンスモジュール内にメモリ１４１２を設ける必要がないので、製造コストが低減されるという利点がある。

ここで、メモリカード１１０に対する動作として、メモリ１４１２中に保持されているコンテンツデータをそのままの状態に保持して、さらに異なるコンテンツデータを追加して記録する動作を「追記」と呼び、メモリ１４１２中に含まれるコンテンツデータ等を消去する動作または再生できる状態にする動作を「消去」と呼ぶ。

以下の表１は、図２に示した第１の保守情報保持部１５２０中に保持される上記追記動作および消去動作を制御するための追記フラグおよびメディア消去フラ

グの状態と、それに対応するメモリカードの動作状態との関係を説明する表である。

表１

メディア単位の管理

保守情報＼値	1	0
追記フラグ	追記可能	追記禁止
メディア消去フラグ	消去可能	消去禁止

すなわち、第１の保守情報保持部１５２０中に保持される追記フラグが「１」である場合は、メモリ１４１２中に保持されたコンテンツデータに加えて、さらに新たなコンテンツデータの書込を行なうことが許可されており、追記フラグが「０」である場合はこのような追記動作が禁止されている。

一方、第１の保守情報保持部１５２０に保持されるメディア消去フラグが「１」である場合は、このメモリカード１１０に対してメモリ１４１２に保持されたデータを外部からの指示に応じて消去することが可能であるのに対し、メディア消去フラグが「０」である場合はこのような消去動作は一切禁止されている。

一方、メモリカード１１０は、外部から与えられる指示に応じて、コントローラ１４２０の制御の下、メモリ１４１２中に保持された各コンテンツデータごとの処理を制御するための保守情報を第２の保守情報保持部１５４０が保持している。

以下では、コンテンツデータごとの再生処理を特に「コンテンツ再生」と呼び、コンテンツデータごとの消去動作を特に「コンテンツ消去」と呼ぶことにする。

表２は、第２の保守情報保持部１５４０が保持するデータと、メモリカード１１０のコントローラ１４２０による制御状態との関係を示す表である。

表２

コンテンツデータ単位の管理

値 / 保守情報	1	0
コンテンツ再生フラグ	再生可能	再生禁止*
コンテンツ消去フラグ	消去可能	消去禁止

*）携帯電話機におけるユーザＩＤが同一の場合は再生可能

すなわち、第２の保守情報保持部１５４０が各コンテンツデータごとに対応して保持するコンテンツ再生フラグが「１」である場合は、対応するコンテンツデータは再生可能状態であり、コンテンツ再生フラグが「０」である場合は原則として当該コンテンツデータの再生は禁止される。

ただし、以下に説明するようにコンテンツ再生フラグが「０」である場合であっても、携帯電話機１００のユーザＩＤデータとメモリカードのユーザＩＤデータとが一致する場合は、当該コンテンツデータの再生動作が許可される。

一方、第２の保守情報保持部１５４０においてコンテンツデータごとに対応して保持されるコンテンツ消去フラグが「１」である場合は、当該コンテンツデータに関しては消去動作が許可されており、コンテンツ消去フラグが「０」である場合は当該コンテンツデータに対する消去動作が禁止されている。

以上のように、メモリカードごとおよびコンテンツデータごとに予め保守情報を設定しておくことで、正規ユーザ以外の者がメモリカード１１０内に保持されたコンテンツデータに対する処理を行なうことを制限し、当該メモリカードのユーザが正当な対価の下に購入したコンテンツデータを保護することが可能となる。

［配信システムの全体構成］

図３は、本発明の記録媒体が用いられる情報配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して、デジタル音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物情報デー

タ、たとえば画像データ等の著作物データを、メモリ等に配信した上でアクセスするあらゆる場合にも適用することが可能なものである。

また、データの配信の方法も携帯電話網による配信に限られるものではなく、たとえば、他の情報通信網を介した配信や、多数のコンテンツデータを蓄えたコンテンツデータ販売機を街頭に設置し、ユーザは、携帯電話機のインターフェースを介して、または、メモリカードに直接にこのコンテンツデータ販売機からコンテンツデータを購入することで、著作物データを入手する構成としても良い。

さらに、暗号化されたコンテンツデータを再生する機器も、携帯電話機に限定されることなく、たとえば、上記メモリカードに対応した専用の再生装置であってもよい。

図３を参照して、著作権の存在する音楽情報を管理する配信サーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、音楽データを配信するための配信キャリアである携帯電話会社２０に、このような暗号化コンテンツデータを与える。一方、認証サーバ１２は、音楽データの配信を求めてアクセスしてきたユーザが正規のユーザであるか否かの認証を行う。

携帯電話会社２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。配信サーバ１０は、配線リクエストがあると、認証サーバ１２によりユーザが正規のユーザであることを確認し、要求された音楽情報をさらに暗号化したうえで、携帯電話会社２０の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

図３においては、たとえば、携帯電話ユーザ１の携帯電話機１００には、携帯電話機１００により受信された暗号化された音楽データを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機１００中の音楽再生部（図示せず）に与えるために、図２において説明したような着脱可能なメモリカード１１０が装着される構成となっている。

さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１２０等を介してこのような再生された音楽データを聴取することが可能である。

以下では、このような配信サーバ１０と認証サーバ１２と配信キャリア（携帯

電話会社）２０とを併せて、音楽サーバ３０と総称することにする。

また、このような音楽サーバ３０から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

このような構成とすることで、まず、メモリカード１１０を購入していない正規のユーザでないものは、音楽サーバ３０からの配信データを受取って再生することが困難な構成となる。

しかも、配信キャリア２０において、たとえば１曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信するたびに発生する著作権料を、配信キャリア２０が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

このとき、たとえばメモリカード１１２を有するユーザ２が、自己の携帯電話機１０２により、音楽サーバ３０から直接音楽データの配信を受けることは可能である。しかしながら、相当量の情報量を有する音楽データ等をユーザ２が直接音楽サーバ３０から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該音楽データの配信を受けているユーザ１から、その音楽情報をコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

図３に示した例では、ユーザ１が受信した音楽データを、デジタル音楽データそのものおよび当該音楽データを再生可能とするために必要な情報とともに、ユーザ２に対してコピーさせる場合を音楽データの「移動」と呼ぶ。この場合、ユーザ１は、再生のために必要な情報（再生情報）ごとユーザ２にコピーさせるため、情報の移動を行なった後には、ユーザ１においては音楽データの再生を行なうことを不可能とする必要がある。ここで、「再生情報」とは、後に説明するように、上記所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なコンテンツキーと、著作権保護に関わる情報であるライセンスＩＤデータやユーザＩＤデータ等のライセンス情報とを意味する。

これに対して、音楽データ（コンテンツデータ）のみを暗号化されたままの状態で、ユーザ２にコピーさせることを音楽情報の「複製」と呼ぶこととする。

この場合、ユーザ２の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされないので、ユーザ２は、コンテンツデータを得ただけでは、音楽情報を再生させることができない。したがって、ユーザ２が、このような音楽情報の再生を望む場合は、改めて音楽サーバ３０からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよいため、ユーザ２が直接音楽サーバ３０からすべての情報の配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

たとえば、携帯電話機１００および１０２が、ＰＨＳ（Personal Handy Phone）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ１からユーザ２への一括した情報の移転（移動）や、コンテンツデータのみの転送（複製）を行なうことが可能である。

［暗号／復号キーの構成］

図４は、図３に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図３に示した構成において、メモリカード１１０内のデータ処理を管理するための鍵としては、メモリカードごとに異なる公開暗号化鍵ＫＰｍｃ（ｎ）と、公開暗号化鍵ＫＰｍｃ（ｎ）により暗号化されたデータを復号するための秘密復号鍵Ｋｍｃ（ｎ）とがある。

ここで、鍵Ｋｍｃ（ｎ）や鍵ＫＰｍｃ（ｎ）の表記中の自然数ｎは、各メモリカードを区別するための番号を表わす。

したがって、メモリカードにおける配信データの授受にあたっては、後に説明するように２つの暗号鍵Ｋｍｃ（ｎ）、ＫＰｍｃ（ｎ）が用いられることになる。

また、メモリカードは、メモリカードのユーザを識別するためのユーザＩＤデータＵｓｅｒ－ＩＤｍを保持している。一方、携帯電話は、携帯電話機のユーザを識別するためのユーザＩＤデータＵｓｅｒ－ＩＤｈを保持している。

さらに、配信されるべきデータについては、まず、音楽データ（コンテンツデ

ータ）自体を暗号化するための共通鍵であるＫｃ（以下、ライセンスキーと呼ぶ）があり、この共通鍵Ｋｃにより暗号化されたコンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンス情報データＬｉｃｅｎｓｅ（ｉ）等が存在する。

このような構成とすることで、ライセンスＩＤデータに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザＩＤデータを用いることで、コンテンツデータの配信を正規に受けたユーザの保護、たとえば、ユーザの許可無く、配信されたコンテンツデータが消去されることを防止するなどの制御を行なうことが可能である。

配信データにおけるコンテンツデータＤｃは、上述のとおり、たとえば音楽情報データであり、このコンテンツデータをライセンスキーＫｃで復号化可能なデータを、暗号化コンテンツデータ［Ｄｃ］Ｋｃと呼ぶ。

［配信サーバ１０の構成］

図５は、図３に示した配信サーバ１０の構成を示す概略ブロック図である。

配信サーバ１０は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したデータや、ライセンスＩＤデータ等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース３０２と、配信情報データベース３０４および課金データベース３０２からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１２と、携帯電話通信網を介して、通信装置３５０により受信されたメモリカードｎからの公開暗号化キーＫＰｍｃ（ｎ）を受取り、配信制御部３１２から与えられる暗号化コンテンツデータを、この公開暗号化キーＫＰｍｃ（ｎ）で更に暗号化してデータバスＢｓ１に与えるための暗号化処理部３２０とを備える。

通信装置３５０は、このようにして暗号化処理部３２０により暗号化されたコンテンツデータを後に説明するように通信網と、配信キャリア２０と、携帯電話網とを介して携帯電話機端末１００等に送信する。

［実施例１の配信処理（保守情報がない場合）］

図６は、図１、図２、図３および図５で説明した情報配信システムにおけるコンテンツデータの配信動作を説明するためのフローチャートである。

図６においては、ユーザ１が、メモリカード１１０を用いることで、音楽サーバ３０から音楽データの配信を受ける場合の動作を説明している。

まず、配信動作が開始されると、ユーザ１の携帯電話機１００からユーザによりキーボード１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

配信サーバ３０は、携帯電話機１００からの配信リクエストを受理すると、携帯電話機１００に対して、公開暗号化キーＫＰｍｃ（１）の送信要求を出力する（ステップＳ１０２）。

携帯電話機１００は、サーバ３０からの公開暗号化キーＫＰｍｃ（１）の送信要求を受信すると（ステップＳ１０４）、カード１１０に対して転送し、カード１１０は、これに応じて、公開暗号化キーＫＰｍｃ（１）を携帯電話機１００に対して出力する（ステップＳ１０６）。

携帯電話機１００は、メモリカード１１０からのキーデータＫＰｍｃ（１）を受けると、サーバ３０に対してこれを送信する（ステップＳ１０８）。

配信サーバ１０は、携帯電話機１００からのキーＫＰｍｃ（１）を受信すると（ステップＳ１１０）、配信情報データベース３０４からの情報をもとにライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１１２）。

続いて、配信サーバ３０は、配信情報データベース３０４から、コンテンツキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを取得する（ステップＳ１１４）。

続いて配信サーバ３０は、携帯電話機１００へ暗号化コンテンツデータ［Ｄｃ］Ｋｃ

を送信する（ステップＳ１１６）。

携帯電話機１００は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１１８）、メモリカード１１０に転送し、メモリカード１１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２にこのまま格納する（ステップＳ１２０）。

一方、サーバ３０は、コンテンツキーＫｃを配信情報データベースより取得し（ステップＳ１２２）、メモリカード１１０から送信された公開暗号化キーＫＰｍｃ（１）によりこのコンテンツキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅを暗号化して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を生成する（ステップＳ１２４）。

配信サーバ１０から携帯電話機１００へデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）が送信され（ステップＳ１２６）、携帯電話機１００がこれを受信すると（ステップＳ１２８）、メモリカード１１０は携帯電話機１００からこのデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を受取ってメモリ１４１２に格納する（ステップＳ１３０）。

続いて、メモリカード１１０は、秘密復号キーＫｍｃ（１）によりデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を復号し、抽出されたライセンスデータＬｉｃｅｎｓｅをライセンス情報保持部１５００に格納する（ステップＳ１３２）。

ライセンス情報データＬｉｃｅｎｓｅのライセンス情報保持部１５００への格納の終了に応じて、携帯電話機１００から配信サーバ３０に対して配信受理が送信される（ステップＳ１３４）。

サーバ３０は配信受理を受信すると（ステップＳ１３６）、課金データベースに配信情報を記録する（ステップＳ１３８）。

以上のような処理により、サーバ３０からメモリカード１１０に対してコンテンツデータ、ライセンス情報データＬｉｃｅｎｓｅおよびコンテンツキーＫｃが配信される。

［実施例１の再生処理（保守情報による保護のない場合）］

図７は、携帯電話機１００内において、メモリカード１１０に保持された暗号化コンテンツデータから、音楽データを復号化し、音楽として外部に出力するための再生処理を説明するためのフローチャートである。以下の説明では、まず、

上述したような保守情報により再生処理に保護がかかっていない状態の処理のフローを説明する。

なお、以下では、暗号化されたデータを復号化した状態、すなわち、本来の状態に復帰したデータを「平文データ」と呼ぶことにする。

図７を参照して、再生処理が開始されると、まず携帯電話機１００のキーボード１１０８等からユーザ１の指示により、再生リクエストがメモリカード１１０に対して出力される（ステップＳ２００）。

カード１１０においては、この再生リクエストに応じて、コントローラ１４２０は、ライセンス情報保持部１５００に保持されるライセンス情報データに基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップＳ２０２）、再生可能と判断した場合はメモリ１４１２内のライセンス情報データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を秘密復号キーＫｍｃ（１）により復号する（ステップＳ２０４）。

一方、コントローラ１４２０が再生不可能と判断した場合は、処理が終了する（ステップＳ２１６）。

再生可能と判断され、カード１１０において、メモリ１４１２内のデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）が復号処理されることで、コンテンツキーＫｃが抽出されると（ステップＳ２０４）、カード１１０からコンテンツキーＫｃが携帯電話機１００に対して出力される（ステップＳ２０６）。

携帯電話機１００が、コンテンツキーＫｃを受理すると（ステップＳ２０８）、続いて、メモリカード１１０からはメモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］ｋｃが携帯電話機１００に対して出力される（ステップＳ２１０）。

携帯電話機１００においては、音楽再生部１５０８が、メモリカード１１０から与えられたコンテンツキーＫｃにより暗号化コンテンツデータ［Ｄｃ］Ｋｃを復号処理して、平文化された音楽データを生成する（ステップＳ２１２）。

音楽再生部１５０８からの出力は混合部１５１０を経由して、デジタルアナログ変換処理部１５１２に伝達され、デジタルアナログ変換処理部１５１２から

平文化音楽データがアナログ音楽信号として再生出力されて（ステップＳ２１４）、再生処理が終了する（ステップＳ２１６）。

以上の処理により、配信サーバ１０からメモリカード１１０に対して配信された暗号化コンテンツキーに基づいて、音楽の再生処理が行なわれることになる。

［実施例１の移動処理（保守情報による保護のない場合）］

図８および図９は、２つのメモリカード間において、コンテンツデータおよびキーデータの移動を行なう処理を説明するためのフローチャートである。

また、図８および図９においても、まず、保守情報による保護がない場合について説明する。

まず、携帯電話機１０２が送信側であり、携帯電話機１００が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１１０と同様の構成を有するメモリカード１１２が装着されているものとする。

移動動作が開始されると、携帯電話機１０２におけるキータッチ部１１０８等とから、ユーザ２により移動リクエストが指示され（ステップＳ３００）、携帯電話機１０２から携帯電話機１００へ公開暗号化キーＫＰｍｃ（１）の送信要求が送信される（ステップＳ３０２）。

携帯電話機１００が公開暗号化キーＫＰｍｃ（１）の送信要求を受信すると（ステップＳ３０４）、メモリカード１１０は、これに応じて、公開暗号化キーＫＰｍｃ（１）を出力する（ステップＳ３０６）。

携帯電話機１００は、メモリカード１１０からの公開暗号化キーＫＰｍｃ（１）を受取って携帯電話機１０２に対して出力し（ステップＳ３０８）、携帯電話機１０２は、キーＫＰｍｃ（１）を受信すると（ステップＳ３１０）、これをメモリカード１１２に転送する。

メモリカード１１２は、キーデータＫＰｍｃ（１）を受理すると（ステップＳ３１２）、メモリカード１１２のメモリ１４１２中の暗号化コンテンツデータ［Ｄｃ］Ｋｃを携帯電話機１０２に対して出力する（ステップＳ３１４）。

携帯電話機１０２から暗号化コンテンツデータ［Ｄｃ］Ｋｃが携帯電話機１００に対して送信され（ステップＳ３１６）、携帯電話機１００がこれを受信すると（Ｓ３１８）、転送された暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリカード１１０は、メモリカード１１０のメモリ１４１２に格納する（ステップＳ３２０）。

続いて、メモリカード１１２においては、メモリカード１１２のメモリ１４１２内の暗号化されたライセンス情報データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（２）を秘密復号キーＫｍｃ（２）により復号する（ステップＳ３２２）。

続いて、メモリカード１１２は、メモリカード１１０から送信されたメモリカード１１０の公開暗号化キーＫＰｍｃ（１）によりコンテンツキーデータＫｃおよびライセンス情報データＬｉｃｅｎｓｅを暗号化して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を生成し（ステップＳ３２４）、これを携帯電話機１０２に対して出力する（ステップＳ３２６）。

続いて図９を参照して、携帯電話機１０２から携帯電話機１００へ、暗号化されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）が送信されると（ステップＳ３２８）、携帯電話機１００はこれを受信して（ステップＳ３３０）、メモリカード１１０は、転送されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を受理する（ステップＳ３３２）。

続いて、メモリカード１１０は、この受信したデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）をメモリカード１１０のメモリ１４１２に格納し（ステップＳ３３４）、続いて、秘密復号キーＫｍｃ（１）によって、このデータを復号して、抽出されたライセンス情報データＬｉｃｅｎｓｅをライセンス情報保持部１５００に格納する（ステップＳ３３６）。

メモリカード１１０において、ライセンス情報データＬｉｃｅｎｓｅのライセンス情報保持部１５００への格納が完了すると、携帯電話機１００から携帯電話機１０２へ配信受理が送信され（ステップＳ３３８）、携帯電話機１０２において、この配信受理が受信されると（ステップＳ３４０）、メモリカード１１２内のライセンス情報保持部１５００のライセンス情報データＬｉｃｅｎｓｅの消去動作が行なわれる（ステップＳ３４２）。

このメモリカード１１２内におけるライセンス情報データＬｉｃｅｎｓｅの消去が完了し（ステップＳ３４２）、かつ、メモリカード１１２のメモリ１４１２内のデータ消去を行なうか否かの確認をユーザ２が携帯電話機１０２のキータッチ部１１０８を介して行なうと（ステップＳ３４４）、続いて、メモリカード１１２のコントローラ１４２０はメモリ内のデータ消去を行なうか否かの判断を行

ない（ステップＳ３４６）、ステップＳ３４４において、メモリ１４１２内のデータ消去が確認されている場合、メモリカード１１２のメモリ１４１２内のデータ［Ｄｃ］Ｋｃおよび［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（２）の消去動作を行ない（ステップＳ３４８）、処理が終了する（ステップＳ３５０）。

一方、メモリ内のデータ消去が許可されない場合（ステップＳ３４６）、そのまま処理が終了する（ステップＳ３５０）。

メモリ内のデータ消去が許可されていない場合においても、メモリカード１１２内のライセンス情報保持部１５００内のライセンス情報データＬｉｃｅｎｓｅが消去されているので、メモリカード１１２は、新たにコンテンツキーデータＫｃおよびライセンス情報データＬｉｃｅｎｓｅをサーバ３０から配信してもらい、ライセンス情報保持部１５００にライセンス情報を保持しない限り、暗号化コンテンツデータ［Ｄｃ］Ｋｃの再生処理を行なうことはできない。

［ユーザＩＤ、保守情報の変更処理］

図１０は、本発明のメモリカード１１０の保守情報（メディア消去フラグ、追記フラグ、コンテンツ再生フラグ、コンテンツ消去フラグ）またはユーザＩＤデータＵｓｅｒ－ＩＤｍの変更指示の処理を説明するためのフローチャートである。

まず変更処理が開始されると、ユーザは、携帯電話機１００のタッチキー部１０８等から、保守情報またはユーザＩＤデータの変更指示を行なう（ステップＳ４００）。

続いて、メモリカードに、ユーザＩＤデータが登録されているか否かの判断が行なわれ（ステップＳ４０２）、ユーザＩＤデータが登録されている場合、メモリカード１１０のコントローラ１４２０は、携帯電話機１００のユーザＩＤ保持部１１０７から携帯電話機１００に登録されているユーザＩＤデータＵｓｅｒ－ＩＤｈを入手する（ステップＳ４０４）。

続いて、コントローラ１４２０は、携帯電話機１００に登録されているユーザＩＤデータＵｓｅｒ－ＩＤｈの値と、メモリカードのユーザＩＤ保持部１５２０に登録されているユーザＩＤデータＵｓｅｒ－ＩＤｍとの比較を行ない（ステップＳ４０６）、一致している場合は、保守情報またはユーザＩＤの変更を行ない（ステップＳ４０８）、処理が終了する（ステップＳ４１２）。ここで、ユーザ

ＩＤデータの変更とは、すでに登録されているユーザＩＤデータの値を別の値に書きかえることであってもかまわないし、また、すでに登録されているユーザＩＤデータの値を消去することであってもかまわない。また、ユーザＩＤを複数個登録できる場合は、ユーザＩＤデータを追加する構成であっても良い。

また、この場合、保守情報の変更は、第１の保守情報保持部１５２０中のメディア単位の管理データの変更でもかまわないし、第２の保守情報保持部１５４０中のコンテンツデータ単位の管理データ単位の変更でもかまわない。

一方、ステップＳ４０２において、メモリカードにユーザＩＤが登録されていない場合、コントローラ１４２０は、携帯電話機に登録されたユーザＩＤ情報との比較を行なうことなく、保守情報またはユーザＩＤデータの変更処理を行ない（ステップＳ４０８）、処理が終了する（ステップＳ４１２）。

一方、メモリカードにユーザＩＤが登録されている場合において、ステップＳ４０６において、携帯電話機のユーザＩＤとメモリカードのユーザＩＤとが一致しない場合は、コントローラ１４２０から携帯電話機１００に対して変更不可の通知がされ（ステップＳ４１０）、処理が終了する（ステップＳ４１２）。

携帯電話機１００では、変更不可の通知を受けると、ディスプレイ１１１０等を介して、ユーザに対し変更処理が許可されないことを通知する。

［再生処理（保守情報の考慮のある場合）］

図１１は、保守情報の考慮のある場合について、本発明のメモリカードのコンテンツデータＤｃ（ｉ）の再生処理を指示した場合のメモリカード１１０の動作を説明するためのフローチャートであり、保守情報の考慮を行なわない場合の図７と対比される図である。

処理が開始されると、ユーザは携帯電話機１００のタッチキー部１１０８のキー操作等により、複数のコンテンツデータのうちのあるコンテンツデータＤｃ（ｉ）の再生指示を行なう（ステップＳ５００）。

自然数ｉは、メモリカードに記録された複数の音楽データを区別するものである。

メモリカード１１０のコントローラ１４２０は、この再生指示に応じて、ライセンス情報保持部１５００中に保持されたコンテンツデータＤｃ（ｉ）に対応す

るライセンス情報データＬｉｃｅｎｓｅ（ｉ）の内容を確認する（ステップＳ５０２）。たとえば、ライセンス情報データＬｉｃｅｎｓｅ（ｉ）の値により、再生回数が制限されている場合、この制限範囲以内であるならば、再生可能と判断され、処理は次のステップに移行する。

一方、ライセンス情報データＬｉｃｅｎｓｅ（ｉ）により、再生不可が指定されている場合は、コントローラ１４２０は、携帯電話機１００に対して再生不可の通知を出力し（ステップＳ５１２）、処理が終了する（ステップＳ５２０）。

再生可能であると判断された場合、続いて、コントローラ１４２０は、コンテンツデータＤｃ（ｉ）に対するコンテンツデータ単位の保守情報を第２の保守情報保持部１５４０に対して照会し、コンテンツ再生フラグの値を確認する（ステップＳ５０４）。当該コンテンツデータＤｃ（ｉ）に対する再生が可能である状態にコンテンツ再生フラグが設定されている場合、コントローラ１４２０に制御されて、復号処理部１４１６は、メモリ１４１２中に保持されている暗号化されたデータ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）を、秘密復号キーＫｍｃ（１）により復号する（ステップＳ５１４）。

このようにしてコンテンツキーＫｃ（ｉ）が、復号抽出され携帯電話機１００の音楽再生部１５０８に対して出力される（ステップＳ５１６）。

さらに、メモリ１４１２からは暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）が、携帯電話機１００の音楽再生部１５０８に対して出力され（ステップＳ５１８）、処理が終了する（Ｓ５２０）。

一方、ステップＳ５０４において、コンテンツ再生フラグのレベルにより、再生禁止が指示されている場合は、続いて、ユーザＩＤ保持部１５２０中にユーザＩＤが登録されているか否かの判断が行なわれる（ステップＳ５０６）、登録されていない場合、処理はステップＳ５１４に進み、コンテンツキーデータＫｃ（ｉ）の復号抽出および暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）の出力が行なわれる。

これに対して、ユーザＩＤ保持部１５２０中にユーザＩＤが登録されている場合、コントローラ１４２０は、携帯電話機１００のユーザＩＤ保持部１１０７から携帯電話機１００のユーザＩＤデータを取得し（ステップＳ５０８）、携帯電

話機１００に登録されたユーザＩＤデータＵｓｅｒ－ＩＤｈと、メモリカードに登録されているユーザＩＤデータＵｓｅｒ－ＩＤｍの値が一致しているか否かの判断を行なう（ステップＳ５１０）。

携帯電話機１００とメモリカード１１０のユーザＩＤが一致している場合は、処理はステップＳ５１４に移行し、コンテンツキーの抽出および暗号化されたコンテンツデータの出力が行なわれる。

一方、携帯電話機１００とメモリカード１１０のユーザＩＤが一致しない場合（ステップＳ５１０）、コントローラ１４２０は、携帯電話機１００に対して再生不可の通知を行ない（ステップＳ５１２）、処理は終了する（ステップＳ５２０）。

以上のような処理により、コンテンツデータごとに、ライセンス情報データに基づいた著作権保護ならびにユーザＩＤデータや保持情報に基づいたユーザ保護を行なった上で、コンテンツデータ（音楽データ）の再生処理を行なうことが可能となる。

［消去処理］

図１２は、メモリカード１１０中に保持されたコシテンツデータの消去動作を説明するためのフローチャートである。

処理が開始され、ユーザが携帯電話機１００のキータッチ部１１０８等からコンテンツデータＤｃ（ｉ）の消去指示を行なう（ステップＳ６００）。まず、メモリカード１１０のコントローラ１４２０は、メモリカード１１０に対する保守情報を記録した第１の保守情報保持部１５２０中のメディア消去フラグの値を確認する（ステップＳ６０２）。

メディア消去フラグにより、消去可能が指示されている場合処理は次のステップに進み、消去禁止が指示されている場合は、コントローラ１４２０は、携帯電話機１００に対して消去不可の通知を行ない（ステップＳ６１０）、処理は終了する（ステップＳ６１２）。

メディア消去フラグが消去可能を指定している場合、コントローラ１４２０は、さらに、消去が指示されたコンテンツデータＤｃ（ｉ）に対するコンテンツデータ単位の保守情報を第２の保守情報保持部１５４０に対して照会し、コンテンツ

消去フラグの値を確認する（ステップＳ６０４）。

当該コンテンツデータＤｃ（ｉ）の消去可能がコンテンツ消去フラグにより指定されている場合は、処理は次のステップに移行する。一方、消去禁止が指示されている場合は、コントローラ１４２０は、消去不可の通知を携帯電話機１００に対して出力し（ステップＳ６１０）、処理は終了する（ステップＳ６１２）。

コンテンツ消去フラグにより当該コンテンツデータＤｃ（ｉ）の消去可能が指示されている場合は、続いて、コントローラ１４２０は、ライセンス情報保持部１５００中のコンテンツデータＤｃ（ｉ）に対応したライセンス情報データＬｉｃｅｎｓｅ（ｉ）の消去動作を行ない（ステップＳ６０６）、メモリ１４１２中に保持された当該コンテンツデータに対応する暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）およびこれに対応する暗号化されたコンテンツキーおよび暗号化されたライセンス情報データ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）の消去動作を行なって（ステップＳ６０８）、処理が終了する（ステップＳ６１２）。

以上のような処理を行なうことで、メモリカードごとに消去動作が可能か否かの指定ができるとともに、各コンテンツデータ単位で消去動作が許可されるかどうかが保守情報により指定されているので、当該コンテンツデータを配信されたユーザの許可なく、メモリ１４１２中のコンテンツデータが消去されてしまうことを防止することが可能となる。

［移動処理（保守情報を考慮した場合：コンテンツデータの出力側）］

図１３は、保守情報を考慮した場合において、メモリカード１１２を移動元としてコンテンツデータの移動処理を行なう場合の処理の流れを説明するためのフローチャートであり、図８および図９で説明したカード１１２の処理と対比される図である。

処理が開始されると、まず、ユーザは、携帯電話機１０２のキータッチ部１１０８等を介して、コンテンツデータＤｃ（ｉ）の移動指示を行ない（ステップＳ７００）、続いて、メモリカード１１２のコントローラ１４２０は、まず第１の保守情報保持部１５２０に登録されたメディア単位の保守情報を照会して、メディア消去フラグの値を確認する（ステップＳ７０２）。

メディア消去フラグが消去可能を指示している場合は、処理は次のステップに移行し、消去禁止が指示されている場合は、メモリカード１１２のコントローラ１４２０は、携帯電話機１０２に対して移動不可の通知を行なって（ステップＳ７２０）、処理は終了する（ステップＳ７２２）。

メディア消去フラグが消去可能を指示している場合は（ステップＳ７０２）、続いて、メモリカード１１２のコントローラ１４２０は、コンテンツデータＤｃ（ｉ）に対するコンテンツデータ単位の保守情報を第２の保守情報保持部１５４０に対して照会し、コンテンツ消去フラグのレベルを確認する（ステップＳ７０４）。

当該コンテンツデータＤｃ（ｉ）に対する消去禁止が指示されている場合は、コントローラ１４２０は、携帯電話機１０２に対して移動不可を通知して（ステップＳ７２０）、処理は終了する（ステップＳ７２２）。

一方、コンテンツ消去フラグが消去可能を指示している場合は、メモリカード１１２のコントローラ１４２０は、ＫＰｍｃ（１）保持部１４０５から、公開暗号化キーＫＰｍｃ（１）を取得し（ステップＳ７０６）、続いて、メモリ１４１２中に格納されている暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）を携帯電話機１００を介して、移動先のメモリカード１１０に対して出力する（ステップＳ７０８）。

続いて、メモリカード１１２のコントローラ１４２０は、復号処理部１４１６を制御して、メモリ１４１２中に保持されたデータ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｃ（ｉ）］Ｋｍｃ（２）を、自身の秘密復号鍵Ｋｍｃ（２）により復号する（ステップＳ７１０）。

さらに、メモリカード１１２のコントローラ１４２０は、暗号化処理部１４１４を制御して、この復号されたコンテンツキーデータおよびライセンス情報データを、移動先のメモリカード１１０から送信された移動先のメモリカード１１０に対する公開暗号化キーＫＰｍｃ（１）により暗号化して、データ［Ｋｃ（ｉ），Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）を生成して、携帯電話機１０２を介して、移動先のメモリカード１１０に対して出力する（ステップＳ７１２）。

続いて、メモリカード１１２のコントローラ１４２０は、ライセンス情報保持

部１５００中に保持されたコンテンツデータＤｃ（ｉ）に対応したライセンス情報データＬｉｃｅｎｓｅ（ｉ）の消去を行なう（ステップＳ７１４）。

続いて、メモリカード１１２のコントローラ１４２０は、携帯電話機１０２のディスプレイ等を介して、ユーザにメモリ１４１２中のデータ消去を行なうか否かの確認を行ない、ユーザからキータッチ部１１０８等を介して消去が指示された場合は（ステップＳ７１６）、メモリ１４１２中の暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）および暗号化されたコンテンツキーおよびライセンス情報データを消去して（ステップＳ７１８）、処理が終了する（ステップＳ７２２）。

一方、ユーザがメモリ１４１２中のデータ消去を指示しなかった場合は、メモリ１４１２中の暗号化されたコンテンツデータ、暗号化されたコンテンツキーデータおよびライセンス情報データを消去することなく処理が終了する（ステップＳ７２２）。

コンテンツデータの一括した移動の場合と同様に、メモリ１４１２内の暗号化されたコンテンツデータの消去を行なわなかった場合も、ライセンス情報保持部１５００中の当該コンテンツデータＤｃ（ｉ）に対応したライセンス情報データは消去されているので、このままではメモリカード１１０は当該コンテンツデータの再生処理を行なうことはできない。

以上のようにして、コンテンツデータ単位で保守情報を参照しつつ、移動元のメモリカード１１２から移動先のメモリカード１１０に対してコンテンツデータの移動を行なうことが可能となる。

［配信・移動処理（保守情報を考慮した場合：コンテンツデータの受け側）］

図１４は、メモリカード１１０に対して、たとえば、移動動作において受信側となっている場合、保守情報を考慮したときのコンテンツデータの追記を行なう処理を説明するためのフローチャートであり、図８および図９で説明したカード１１０の処理と対比される図である。

コンテンツデータの追記としては、上述のとおり、コンテンツデータをメモリカード間で移動させる場合に受信してもよいし、あるいは、たとえば、携帯電話網を介して配信サーバ１０から配信を受ける構成としてもよいし、街頭に設置さ

れたコンテンツデータ販売機を介して、メモリカードに直接コンテンツデータが書込まれる構成としてもよい。

処理が開始されると、ユーザ2は、携帯電話機１０２のキータッチ部１１０８等を介して、コンテンツデータＤｃ（ｉ）の移動（記録）指示をメモリカード１１０に対して与える（ステップＳ８００）。

続いて、メモリカード１１０のコントローラ１４２０は、メディア単位の保守情報を第１の保守情報保持部１５２０に対して照会し、追記フラグのレベルを確認する（ステップＳ８０２）。追記が禁止されている場合、コントローラ１４２０は、携帯電話機１００に対して移動不可の通知を出力し（ステップＳ８１６）、処理が終了する（ステップＳ８１８）。この移動不可の通知は、携帯電話機１００から携帯電話機１０２にさらに伝達される。

一方、追記フラグにより追記可能が指示されている場合は、メモリカード１１０は、ＫＰｍｃ（１）保持部１４０５から、メモリカード１１０に対する公開暗号化キーＫＰｍｃ（１）を追記に対する移動元（メモリカード１１２）に対して出力し（ステップＳ８０４）、移動元から暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）を受けて、メモリ１４１２に格納する（ステップＳ８０６）。

続いて、メモリカード１１０は、携帯電話機１００を介して、移動元からメモリカード１１０に対する公開暗号化キーＫＰｍｃ（１）により暗号化されたコンテンツキーデータおよびライセンス情報データ［Ｋｃ（ｉ）、Ｌｉｃｅｎｓｅ（ｉ）］Ｋｍｃ（１）を受け、メモリ１４１２に対して格納する（ステップＳ８１０）。

続いて、コントローラ１４２０により制御されて、復号処理部１４１６がメモリ１４１２中に保持されたコンテンツキーデータおよびライセンス情報データを秘密復号キーＫｍｃ（１）により復号し（ステップＳ８１２）、復号されたライセンス情報データＬｉｃｅｎｓｅ（ｉ）をライセンス情報保持部１５００に格納して（ステップＳ８１４）、処理が終了する（ステップＳ８１８）。

以上のような処理を行なうことで、コンテンツデータ単位の追記動作を行なうことが可能となる。

すなわち、第１には、メモリカードにはユーザＩＤデータＵｓｅｒ－ＩＤｍが

保持され、携帯電話機には、ユーザＩＤデータＵｓｅｒ－ＩＤｈが保持される構成とすることで、メモリカードのユーザと携帯電話機のユーザとが一致しないかぎり、保守情報やユーザＩＤデータＵｓｅｒ－ＩＤｍを変更することが出来ないため、正規にコンテンツデータを購入したユーザを保護することが可能となる。

しかも、第２には、再生処理、移動処理、消去処理等において、ユーザの設定した保守情報により、コンテンツデータが正規の購入者に無断で、再生されたり、消去されたり、他のメモリカードに移動されたりすることを防止することが可能となる。

［実施例２］

実施例１のメモリカードでは、メモリカードのユーザと携帯電話機のユーザとが一致しないかぎり、保守情報やユーザＩＤデータＵｓｅｒ－ＩＤｍを変更することが出来ない構成とし、しかも、再生処理、移動処理、消去処理等において、ユーザの設定した保守情報により、コンテンツデータが正規の購入者に無断で、再生されたり、消去されたり、他のメモリカードに移動されたりすることを防止する構成であった。

実施例２のメモリカードでは、さらに、コンテンツデータの移動の制限として、メモリカードのユーザＩＤデータとそれが装着される携帯電話機のユーザＩＤデータの２つのユーザＩＤが一致しない場合には、コンテンツデータに対応したライセンス情報の移動または消去が禁止される。

まず、実施例１と同様に、ユーザＩＤデータＵｓｅｒ－ＩＤｍをメモリカード１１０のユーザＩＤ保持部１５２０が記録し、携帯電話機１００においてもユーザＩＤ保持部１１０７にユーザＩＤデータＵｓｅｒ－ＩＤｈを記録しているものとする。

図１５は、このような構成を有する携帯電話機１００が、メモリカード１１０を装着した状態で、配信サーバ１０および配信キャリア（携帯電話会社）２０を介して、コンテンツデータの配信を受ける状態を示す概念図である。

図１５に示した構成では、ｉ番目のコンテンツデータＤｃ（ｉ）に対する再生情報Ｒｅａｄ（ｉ）として、コンテンツ復号キーＫｃ（ｉ）、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ（ｉ）およびコンテンツデータの配信を受けた際のユ

ーザを示すユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）の組合せを用いた場合の構成を示す。

ここで、このコンテンツデータごとに対応し、ライセンス情報中に含まれるユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）は、当該コンテンツデータ配信の際にユーザＩＤデータＵｓｅｒ－ＩＤｈの値が転写される。

配信サーバ１０から携帯電話網を介して暗号化されたコンテンツデータＤｃ（ｉ）が配信された場合、携帯電話機に記録されているユーザＩＤデータＵｓｅｒ－ＩＤｈは“０９０００００００１”であり、かつ、メモリカード１１０中に保持されるユーザＩＤデータＵｓｅｒ－ＩＤｍも“０９０００００００１”という値が保持されているものとする。このとき、コンテンツデータＤｃ（ｉ）に対応した再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）も“０９０００００００１”であるものとする。

再生情報Ｒｅａｄ（ｉ）は、暗号化キーＫＰｍｃ（１）により暗号化されたデータ［Ｒｅａｄ（ｉ）］Ｋｍｃ（１）として、メモリカード１１０中のメモリ１４１２に保持されているものとする。

さらに、メモリカード１１０のメモリ１４１２中には暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）が保持されている。

図１６は、２つのメモリカード１１０と１１２との間で、再生情報の移動が許可される場合を示す概念図である。

図１６に示した場合は、送信元の携帯電話機１００では、メモリカード１１０のユーザＩＤデータＵｓｅｒ－ＩＤｍと、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈとが一致している。

このような場合には、メモリカード１１０からメモリカード１１２に対して、暗号化コンテンツデータのみならず暗号化再生情報Ｒｅａｄ（ｉ）の移動が許可されて、暗号化されたコンテンツデータ［Ｄｃ（ｉ）］Ｋｃ（ｉ）を携帯電話機１０２の側でも再生することが可能になる。メモリカード１１０のライセンス情報保持部１５００からは、実施例１と同様に、暗号化コンテンツデータと再生情報の双方がメモリカード１１２に移動するのに伴なって、再生情報が消去される。

図１７は、２つのメモリカード１１０と１１２との間で、再生情報の移動が許

可されない場合を示す概念図である。

送信元の携帯電話機１００では、メモリカード１１０のユーザＩＤデータＵｓｅｒ－ＩＤmと、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈとは一致していない。

したがって、このような場合は、メモリカード１１０のコントローラ１４２０は、メモリカード１１０のメモリ１４１２中の再生情報Ｒｅａｄ（ｉ）のメモリカード１１２への転送を許可しない。

このような構成とすることで、正規のユーザ以外が、無断でコンテンツデータを他のメモリカードに移動することを禁じることが可能となる。

再生情報としてはコンテンツキー（暗号化コンテンツデータの復号キー）のみを含む構成としてもよいし、コンテンツキーとライセンス情報データとの組合せとしてもよい。

ただし、再生情報をコンテンツキーとユーザＩＤデータとした場合、または、コンテンツ復号キー、ライセンス情報データおよびユーザＩＤデータの組合せとした場合は、以下のような処理を行なうことが可能である。

すなわち、以上の説明では、携帯電話機のユーザＩＤデータとメモリカードのユーザＩＤデータとの一致／不一致に応じて、コンテンツデータに対応したライセンス情報の移動または消去が禁止される構成であった。

上述のとおり、再生情報Ｒｅａｄ（ｉ）として、言いかえると、コンテンツデータごとに、ユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）がライセンス情報保持部１５００およびメモリ１４１２に格納されている場合は、このユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）の値と、メモリカードのユーザＩＤデータＵｓｅｒ－ＩＤmの値、携帯電話機のユーザＩＤデータＵｓｅｒ－ＩＤｈの値とに応じて、再生情報の移動を許可するか否かを、コンテンツデータごとに判断して、処理することが可能である。

すなわち、メモリカードに記録された再生情報に含まれるユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）と、メモリカードのユーザＩＤデータＵｓｅｒ－ＩＤmと携帯電話機に記憶されたユーザＩＤデータＵｓｅｒ－ＩＤｈとの関係から、コンテンツデータのライセンス情報の移動または消去が禁止されるという制御を行なう

ことが可能である。

図１８は、このようにコンテンツデータ単位で、再生情報の転送を制御する場合の構成を示す概念図である。

なお、実施例１の図１０で説明したのと同様に、携帯電話機のユーザＩＤデータＵｓｃｒ－ＩＤｈとメモリカードのユーザＩＤデータＵｓｅｒ－ＩＤｍと、コンテンツデータＤｃ（ｉ）に対応したユーザ情報データ中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）とが一致している場合にユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）を書きかえることで、ユーザＩＤに対する制限を解除することが可能である。また、コンテンツデータＤｃ（ｉ）に対応したユーザ情報データ中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）が記憶されていない場合は、ユーザＩＤに対する制限は、働かないものとする。

以上のような構成とした場合、メモリカード１１０からメモリカード１１２へ再生情報の移動が行なわれた後の状態としては、たとえば、以下の５通りのような場合がある。

まず、図１８においても、図１５と同様に、ｉ番目のコンテンツデータＤｃ（ｉ）に対する再生情報Ｒｅａｄ（ｉ）として、コンテンツ復号キーＫｃ（ｉ）、ライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ（ｉ）およびコンテンツデータの配信を受けた際のユーザを示すユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）の組合せを用いる。

また、携帯電話機１００に記録されているユーザＩＤデータＵｓｅｒ－ＩＤｈは“０９０００００００１”であり、かつ、メモリカード１１０中に保持されるユーザＩＤデータＵｓｅｒ－ＩＤｍも“０９０００００００１”という値が保持されているものとする。携帯電話機１０２に記録されているユーザＩＤデータＵｓｅｒ－ＩＤｈは“０９０００００００２”であり、かつ、メモリカード１１２中に保持されるユーザＩＤデータＵｓｅｒ－ＩＤｍも“０９０００００００２”という値が保持されているものとする。

さらに、再生情報Ｒｅａｄ（ｉ）は、暗号化キーＫＰｍｃ（１）により暗号化されたデータ［Ｒｅａｄ（ｉ）］Ｋｍｃ（１）として、メモリカード１１０中のメモリ１４１２に保持されているものとする。

図１８を参照して、まず、第１の場合としては、メモリカード１１０において、コンテンツデータＤｃ（ｉ）に対応した再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）も“０９０００００００１”であるものとする。この場合、メモリカード１１０のユーザＩＤデータＵｓｅｒ－ＩＤmと携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈが一致し、かつ、コンテンツデータＫｃ（ｉ）に対応したユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）もこれらと一致するので、再生情報の移動が許可され、かつ、メモリカード１１２に移動後も、再生情報Ｒｅａｄ（ｊ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｊ）は“０９０００００００１”のままである。

第２の場合としては、上記第１の場合の移動後に、携帯電話機１０２において、再生情報Ｒｅａｄ（ｊ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｊ）を“０９０００００００２”にした場合である。

第３の場合としては、上記第１の場合の移動後に、携帯電話機１０２において、再生情報Ｒｅａｄ（ｊ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｊ）を消去した場合である。

第４の場合としては、もともと、再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）は記録されていない場合である。この場合は、再生情報の移動が許可され、ユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）による移動の制限はない。

第５の場合は、第４の場合において、さらにユーザが携帯電話機１０２の側で、再生情報Ｒｅａｄ（ｊ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｊ）を“０９０００００００２”とした場合である。

以上、第１から第５のいずれの場合も、メモリカード１１０のライセンス情報保持部１５００からは、暗号化コンテンツデータと再生情報の双方がメモリカード１１２に移動するのに伴なって、再生情報が消去される。

図１９は、これらに対して、このようにコンテンツデータ単位で、再生情報の転送を制御した場合に、ライセンス情報の移動が禁止されるときを示す概念図である。

移動元の携帯電話機１００においては、メモリカード１１０のユーザＩＤデー

タＵｓｅｒ－ＩＤｍと、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈとは一致しているものの、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈと再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）とが一致しないため、再生情報の移動が禁止される。

このような構成により、メモリカードという携帯電話機から着脱可能な記録媒体に暗号化コンテンツデータと、これを復号して再生するための情報とが記録されている場合に、正規のユーザ以外が、無断でデータの移動等を行なうことを防止することが可能となる。

なお、携帯電話機のユーザＩＤデータは、携帯電話機であればその電話番号あるいは利用者によって決められたニックネーム、暗証番号とこれらの組合せ等を用いることが可能である。

ライセンス情報としてはコンテンツキー（暗号化コンテンツデータの復号キー）のみを含む構成としてもよいし、コンテンツキーとライセンスＩＤ情報（再生に関する権利情報）との組合せとしてもよい。また、コンテンツキーとユーザＩＤデータとしてもよいし、コンテンツキー、ライセンス情報データおよびユーザＩＤデータの組合せとしてもよい。更に、再生に係わる情報があれば、いかなるデータが追加されていても良い。

また、実施例２においても、実施例１の図１０で説明したのと同様にして、メモリカード中のユーザＩＤデータＵｓｅｒ－ＩＤｍだけでなく保守情報の変更を行う構成とすることが可能である。

このとき、実施例１と同様に、メモリカードにユーザＩＤデータＵｓｅｒ－ＩＤｍが登録されていない場合は、上記ユーザＩＤデータＵｓｅｒ－ＩＤｍや保守情報の変更や、暗号化コンテンツデータの再生動作は、メモリカードのユーザＩＤデータＵｓｅｒ－ＩＤｍには制限を受けない構成とすることができる。

なお、以上説明してきた各実施例において、コンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作情報や音楽サーバ３０に対するアクセス情報等を、付加情報Ｄｉとして暗号化コンテンツデータと併せて配信することも可能である。この付加データＤｉは、配信、移動、

複製においてはコンテンツデータとともに処理され、再生時には分離されて音楽データとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ１４１２に記録される。

なお、以上の説明では、メモリカードとしての構成を説明したが、本発明はこのような構成に限定されることなく、より一般に、配信された暗号化コンテンツデータを再生出力する再生装置、たとえば、携帯電話機に対して着脱可能であって、かつ、暗号化コンテンツデータの配信のために必要なキーデータ等の授受を行う機能を有して、この暗号化コンテンツデータを受けて記録する装置に対して適用可能なものである。

さらに、本発明において、ユーザが音楽データなどのコンテンツデータを入手する経路としては、上述のとおり、携帯電話網や他の情報通信網を介したデータ配信に限られるものではなく、たとえば、多数のコンテンツデータを蓄えて街頭に設置されたコンテンツデータ販売機などにより販売される情報を記録する記録装置にも適用可能なものである。

この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となってはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

請求の範囲

1．暗号化コンテンツデータを再生出力する再生装置に対して着脱可能であって、前記暗号化コンテンツデータを受けて記録するための記録装置であって、

外部との間でデータの授受を可能とするためのデータ入出力部（１２０２）と、

前記データ入出力部からの前記暗号化コンテンツデータを格納するための第１の記憶部（１４１２）と、

前記記録装置のユーザを識別するための第１のユーザ特定データを保持するためのユーザ情報保持部（１５３０）と、

外部から与えられるユーザ情報と前記第１のユーザ特定データとの比較結果に応じて外部からの指示により更新可能な保護情報を保持する保護情報保持部と、

前記記録装置の動作を制御するための制御部（１４２０）とを備え、

前記制御部は、前記保護情報に基づいて、外部からの前記第１の記憶部に保持された前記暗号化コンテンツデータに対するアクセスを制限する、記録装置。

2．前記制御部は、外部から与えられるユーザ情報と前記第１のユーザ特定データとが一致する場合に、前記ユーザ特定データの変更を可能とする、請求項１記載の記録装置。

3．前記制御部は、前記ユーザ情報保持部に前記第１のユーザ特定データが未登録の場合に、前記保護情報の変更および前記ユーザ特定データの変更を可能とする、請求項２記載の記録装置。

4．前記保護情報保持部は、

前記保護情報のうち、前記記録装置自体に対するアクセスの制限に対する第１の保守情報を保持する第１の保守情報保持部（１５２０）を含み、

前記制御部は、前記第１の保守情報に応じて、前記第１の記憶部に対して、新たな暗号化コンテンツデータの追記を禁止する、請求項１記載の記録装置。

5．前記保護情報保持部は、

前記保護情報のうち、前記記録装置自体に対するアクセスの制限に対する第１の保守情報を保持する第１の保守情報保持部を含み、

前記制御部は、前記第１の保守情報に応じて、前記第１の記憶部に対して、新

たな暗号化コンテンツデータの消去を禁止する、請求項１記載の記録装置。

６．前記保護情報保持部は、

前記保護情報のうち、前記暗号化コンテンツデータごとのアクセスの制限に対する第２の保守情報を保持する第２の保守情報保持部（１５４０）をさらに含み、

前記制御部は、前記第１および第２の保守情報に応じて、前記第１の記憶部に保持され、前記第２の保守情報に対応する暗号化コンテンツデータの消去を禁止する、請求項５記載の記録装置。

７．前記保護情報保持部は、

前記保護情報のうち、前記暗号化コンテンツデータごとのアクセスの制限に対する第２の保守情報を保持する第２の保守情報保持部を含み、

前記制御部は、前記第２の保守情報に応じて、前記第１の記憶部に保持され、前記第２の保守情報に対応する暗号化コンテンツデータの消去を禁止する、請求項１記載の記録装置。

８．前記制御部は、外部から前記暗号化コンテンツデータの再生動作が指示された場合、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項６記載の記録装置。

９．前記制御部は、外部から与えられるユーザ情報と前記第１のユーザ特定データとが一致する場合に、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項８記載の記録装置。

１０．前記制御部は、前記ユーザ情報保持部に前記第１のユーザ特定データが未登録の場合に、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項８記載の記録装置。

１１．前記制御部は、外部から与えられるユーザ情報と前記第１のユーザ特定データとが一致する場合に、前記第１および第２の保守情報のうち、少なくとも１つの保守情報を書きかえることを許可する、請求項４記載の記録装置。

１２．前記制御部は、前記ユーザ情報保持部に前記第１のユーザ特定データが未

登録の場合に、前記第１および第２の保守情報のうち、少なくとも１つの保守情報を書きかえることを許可する、請求項４記載の記録装置。

１３．前記記録装置は、

前記暗号化コンテンツデータにそれぞれ対応し、前記暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第２の記憶部（１５００）をさらに備え、

前記制御部は、外部から前記第１の記憶部に保持された前記暗号化コンテンツデータの移動が指示された場合、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データとの比較結果に応じて、前記第２の記憶部を制御して、前記ライセンス情報データを前記データ入出力部に与える、請求項１記載の記録装置。

１４．前記記録装置は、

前記暗号化コンテンツデータにそれぞれ対応し、前記暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第２の記憶部をさらに備え、

前記ライセンス情報の各々は、前記暗号化コンテンツデータごとに対応するコンテンツユーザ特定データを含み、

前記制御部は、外部から前記第１の記憶部に保持された前記暗号化コンテンツデータの移動が指示された場合、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データと、前記コンテンツユーザ特定データとの比較結果に応じて、前記第２の記憶部を制御して、前記暗号化コンテンツデータごとに前記ライセンス情報データを前記データ入出力部に与える、請求項１記載の記録装置。

１５．前記制御部は、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データとの比較結果に応じて、前記コンテンツユーザ特定データの変更を許可する、請求項１４記載の記録装置。

１６．前記コンテンツユーザ特定データは、対応する前記暗号化コンテンツデータの配信の際に前記ユーザ情報保持部に保持される前記第１のユーザ特定データ

である、請求項１４記載の記録装置。

１７．前記制御部は、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データとの比較結果に応じて、前記コンテンツユーザ特定データの変更を許可する、請求項１６記載の記録装置。

１８．前記第１の記憶部は、半導体メモリであり、

前記記録装置は、メモリカードである、請求項１記載の記録装置。

10/069119
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 900393	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP00/05833	International filing date (*day/month/year*) 29 August 2000 (29.08.00)	Priority date (*day/month/year*) 30 August 1999 (30.08.99)

International Patent Classification (IPC) or national classification and IPC
G06F 17/60, G06K 19/00, 19/10, H04H 1/00, H04L 9/32, H04M 3/42, 3/493, 11/08

Applicant
FUJITSU LIMITED

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 10 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
09 March 2001 (09.03.01)	28 December 2001 (28.12.2001)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

rnational application No.
PCT/JP00/05833

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-31, 33, as originally filed

pages _____, filed with the demand

pages 32, filed with the letter of 24 August 2001 (24.08.2001)

☒ the claims:

pages 1-10, 13-18, as originally filed

pages _____, as amended (together with any statement under Article 19

pages _____, filed with the demand

pages 11-12, filed with the letter of 24 August 2001 (24.08.2001)

☒ the drawings:

pages 1-5, 7-12, 14, as originally filed

pages _____, filed with the demand

pages 6, 13, 15-19, filed with the letter of 24 August 2001 (24.08.2001)

☐ the sequence listing part of the description:

pages _____, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP 00/05833

V. **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims		NO
Inventive step (IS)	Claims	1-18	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

Document 1: JP, 10-269144, A (Sony Corp.), October 9, 1998

Document 2: JP, 10-283268, A (Toshiba Corp.), October 23, 1998

Document 3: JP, 5-197635, A (Fujitsu Ltd.), August 6, 1993

Document 4: JP, 11-259964, A (Sony Corp.), September 24, 1999

Claims 1 to 18

Documents 1 and 2 are documents that reflect the general state of the art in this technical field. Document 1 discloses the feature wherein, by adding restriction information relating to restricting the number of times and when operations such as the reproduction or copying of information can be performed, illegal copying of information can be prevented and information can be shared and transmitted. Document 2 discloses the feature wherein, when decrypting information that has been encrypted, certain conditional information is recorded to prevent illegal copying.

However, "a recording device provided with a maintenance information holding part for maintenance information that can be renewed by instructions from the

outside in response to a comparison between the user information obtained from the outside and the first user ID data, and which restricts access from the outside to the encrypted contents data retained in the first memory" is neither disclosed nor suggested in Documents 1 to 4 cited in the international search report. Moreover, it is not obvious to a person skilled in the art.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

(1) Lines 15 and 16 on page 15 of the description state as an explanation for Step S132 "data [Kc, License] Kmc (1) is decrypted using the secret decryption key Kmc (1)". However, Fig. 6 indicates that in Step S132 "{Kc, License} Ks is decrypted using Kmc(1)". Consequently, the terminology used is not consistent throughout the international application.

(2) Lines 26 and 27 on page 7 of the description state "the operation of deleting content data and the like, and the operation of rendering a state in which reproduction is possible are called "deletion". However, with the exception of this disclosure, there are no other explanations given with respect to "the operation of rendering a state in which reproduction is possible", thereby this configuration is unclear. Moreover, calling "the operation of rendering a state in which reproduction is possible" "deletion" is inappropriate.

EP・US　　特許協力条約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　９００３９３	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０５８３３	国際出願日（日.月.年）　２９．０８．００	優先日（日.月.年）　３０．０８．９９
出願人（氏名又は名称）　富士通株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　4　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☒ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　2　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報[redacted]

国際出願番[redacted]PCT／JP00／05833

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☒ 請求の範囲 11-12 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
請求の範囲１１－１２において、「前記第１および第２の保守情報」と記載されているが、引用している請求の範囲４及び１には第１の保守情報に関する記載のみがあり、第２の保守情報に関する記載はなく、不明確である。

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意
☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

国際調査報[redacted]　　国際出願番号[redacted]PCT／JP00／05833

A.　発明の属する分野の分類（国際特許分類（IPC））
IntCl⁷　G06F 17／60, G06K 19／00, G06K 19／10,
H04H 1／00, H04L 9／32,
H04M 3／42, H04M 3／493, H04M 11／08

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
IntCl⁷　G06F 17／60, G06K 17／00, G06K 19／00－19／10,
H04H 1／00, H04L 9／32,
H04M 3／42, H04M 3／493, H04M 11／08

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案広報　1922－1996年
日本国公開実用新案広報　1971－2000年
日本国登録実用新案広報　1994－2000年
日本国実用新案登録広報　1996－2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP, 10－269144, A（ソニー株式会社） 9．10月．1998（09．10．98） 全文、全図（ファミリーなし）	1-10, 13-18
A	JP, 10－283268, A（株式会社東芝） 23．10月．1998（23．10．98） 全文、全図（ファミリーなし）	1-10, 13-18

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
19．12．00	26.12.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	相崎　裕恒 電話番号　03－3581－1101　内線　3585	5N　2945

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報[redacted]　　国際出願番号[redacted]ＰＣＴ／ＪＰ００／０５８３３

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ，５－１９７６３５，Ａ（富士通株式会社） ６．８月．１９９３（０６．０８．９３） 全文、全図（ファミリーなし）	1-10, 13-18
Ｐ，Ａ	ＪＰ，１１－２８３２６８，Ａ（株式会社東芝） ２４．９月．１９９９（２４．０９．９９） 全文、全図（ファミリーなし）	1-10, 13-18

97

特　許　協　力　条　約

RECD 08 FEB 2002

PCT

国際予備審査報告

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　９００３９３	今後の手続きについては、国際予備審査報告の送付通知（様式ＰＣＴ／ＩＰＥＡ／４１６）を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０５８３３	国際出願日（日.月.年）　２９．０８．００	優先日（日.月.年）　３０．０８．９９
国際特許分類（ＩＰＣ）　Ｉｎｔ．Ｃｌ．' Ｇ０６Ｆ １７／６０，Ｇ０６Ｋ １９／００，Ｇ０６Ｋ １９／１０，Ｈ０４Ｈ １／００，Ｈ０４Ｌ ９／３２，Ｈ０４Ｍ ３／４２，Ｈ０４Ｍ ３／４９３，Ｈ０４Ｍ １１／０８		
出願人（氏名又は名称）　富士通株式会社		

１．　国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

２．　この国際予備審査報告は、この表紙を含めて全部で　４　ページからなる。

☒　この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び／又は図面も添付されている。
（ＰＣＴ規則70.16及びＰＣＴ実施細則第６０７号参照）
この附属書類は、全部で　１０　ページである。

３．　この国際予備審査報告は、次の内容を含む。

- Ⅰ　☒　国際予備審査報告の基礎
- Ⅱ　☐　優先権
- Ⅲ　☐　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
- Ⅳ　☐　発明の単一性の欠如
- Ⅴ　☒　ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
- Ⅵ　☐　ある種の引用文献
- Ⅶ　☒　国際出願の不備
- Ⅷ　☐　国際出願に対する意見

国際予備審査の請求書を受理した日　０９．０３．０１	国際予備審査報告を作成した日　２８．１２．０１
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｎ　２９４５ 奥村　元宏 電話番号　０３－３５８１－１１０１　内線　６９１５

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（１９９８年７月）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ００／０５８３３

Ⅰ．　国際予備審査報告の基礎

1．　この国際予備審査報告は下記の出願書類に基づいて作成された。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。ＰＣＴ規則70.16, 70.17）

☐ 出願時の国際出願書類

☒ 明細書　第 1-31, 33 ページ、　出願時に提出されたもの
明細書　第 　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書　第 32 ページ、　２４．０８．０１ 付の書簡と共に提出されたもの

☒ 請求の範囲　第 1-10, 13-18 項、　出願時に提出されたもの
請求の範囲　第 　　項、　ＰＣＴ１９条の規定に基づき補正されたもの
請求の範囲　第 　　項、　国際予備審査の請求書と共に提出されたもの
請求の範囲　第 11-12 項、　２４．０８．０１ 付の書簡と共に提出されたもの

☒ 図面　第 1-5, 7-12, 14 ページ/~~図~~、　出願時に提出されたもの
図面　第 　　ページ/~~図~~、　国際予備審査の請求書と共に提出されたもの
図面　第 6, 13, 15-19 ページ/~~図~~、　２４．０８．０１ 付の書簡と共に提出されたもの

☐ 明細書の配列表の部分　第 　　ページ、　出願時に提出されたもの
明細書の配列表の部分　第 　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分　第 　　ページ、　　付の書簡と共に提出されたもの

2．　上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である 　　語である。

☐ 国際調査のために提出されたＰＣＴ規則23.1(b)にいう翻訳文の言語
☐ ＰＣＴ規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたＰＣＴ規則55.2または55.3にいう翻訳文の言語

3．　この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出された書面による配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4．　補正により、下記の書類が削除された。
☐ 明細書　第 　　ページ
☐ 請求の範囲　第 　　項
☐ 図面　図面の第 　　ページ／図

5．☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)　この補正を含む差し替え用紙は上記１．における判断の際に考慮しなければならず、本報告に添付する。）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ００／０５８３３

Ⅴ．　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（Ｎ）	請求の範囲	１－１８	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲	１－１８	有
	請求の範囲		無
産業上の利用可能性（ＩＡ）	請求の範囲	１－１８	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：ＪＰ　１０－２６９１４４　Ａ（ソニー株式会社）
　　１９９８．１０．０９
文献２：ＪＰ　１０－２８３２６８　Ａ（株式会社東芝）
　　１９９８．１０．２３
文献３：ＪＰ　５－１９７６３５　Ａ（富士通株式会社）
　　１９９３．０８．０６
文献４：ＪＰ　１１－２５９９６４　Ａ（ソニー株式会社）
　　１９９９．０９．２４

請求の範囲１－１８

上記文献１、２は、当該技術分野における一般的な技術水準を示す文献であって、上記文献１には、情報の再生やコピー等の操作を制限する回数や時間などに関する制限情報を付加することにより、情報の違法コピーを防止すると共に、情報の共有や伝達を行う技術が記載されており、上記文献２には、暗号化された情報に復号化する際の条件情報を記録し、不正コピーを防止する技術が記載されている。

しかし、「外部から与えられるユーザ情報と第１のユーザ特定データとの比較結果に応じて外部からの指示により更新可能な保護情報を保持する保護情報保持部を備え、保護情報に基づいて、外部からの第１の記憶に保持された暗号化コンテンツデータに対するアクセスを制限する記録装置」に関しては、国際調査報告で列記した上記文献１－４のいずれにも、記載も示唆もされていない。

Ⅶ.　国際出願の不備

この国際出願の形式又は内容について、次の不備を発見した。

（１）明細書第１５頁第１５－１６行目には、ステップＳ１３２の説明として「秘密復号キーＫｍｃ（１）によりデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｍｃ（１）を復号し、」と記載されているが、第６図において、ステップＳ１３２には「Ｋｍｃ（１）にて｛Ｋｃ、Ｌｉｃｅｎｓｅ｝Ｋｓを復号」と示されている。したがって、用語が国際出願の全体を通じて一貫して使用されていない。

（２）明細書第７頁第２６－２７行目には、「コンテンツデータ等を消去する動作または再生できる状態にする動作を「消去」と呼ぶ。」と記載されているが、”再生できる状態にする動作”に関してはこの記載以外に説明がなく、いかなる構成であるのか不明である。また、”再生できる状態にする動作”を「消去」と呼ぶのは不適切である。

タＵｓｅｒ－ＩＤｍと、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈとは一致しているものの、携帯電話機１００のユーザＩＤデータＵｓｅｒ－ＩＤｈと再生情報Ｒｅａｄ（ｉ）中のユーザＩＤデータＵｓｅｒ－ＩＤ（ｉ）とが一致しないため、再生情報の移動が禁止される。

このような構成により、メモリカードという携帯電話機から着脱可能な記録媒体に暗号化コンテンツデータと、これを復号して再生するための情報とが記録されている場合に、正規のユーザ以外が、無断でデータの移動等を行なうことを防止することが可能となる。

なお、携帯電話機のユーザＩＤデータは、携帯電話機であればその電話番号あるいは利用者によって決められたニックネーム、暗証番号とこれらの組合せ等を用いることが可能である。

再生情報としてはコンテンツキー（暗号化コンテンツデータの復号キー）のみを含む構成としてもよいし、コンテンツキーとライセンスＩＤ情報（再生に関する権利情報）との組合せとしてもよい。また、コンテンツキーとユーザＩＤデータとしてもよいし、コンテンツキー、ライセンス情報データおよびユーザＩＤデータの組合せとしてもよい。更に、再生に係わる情報があれば、いかなるデータが追加されていても良い。

また、実施例２においても、実施例１の図１０で説明したのと同様にして、メモリカード中のユーザＩＤデータＵｓｅｒ－ＩＤｍだけでなく保守情報の変更を行う構成とすることが可能である。

このとき、実施例１と同様に、メモリカードにユーザＩＤデータＵｓｅｒ－ＩＤｍが登録されていない場合は、上記ユーザＩＤデータＵｓｅｒ－ＩＤｍや保守情報の変更や、暗号化コンテンツデータの再生動作は、メモリカードのユーザＩＤデータＵｓｅｒ－ＩＤｍには制限を受けない構成とすることができる。

なお、以上説明してきた各実施例において、コンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作情報や音楽サーバ３０に対するアクセス情報等を、付加情報Ｄｉとして暗号化コンテンツデータと併せて配信することも可能である。この付加データＤｉは、配信、移動、

たな暗号化コンテンツデータの消去を禁止する、請求項１記載の記録装置。

６．前記保護情報保持部は、

前記保護情報のうち、前記暗号化コンテンツデータごとのアクセスの制限に対する第２の保守情報を保持する第２の保守情報保持部（１５４０）をさらに含み、

前記制御部は、前記第１および第２の保守情報に応じて、前記第１の記憶部に保持され、前記第２の保守情報に対応する暗号化コンテンツデータの消去を禁止する、請求項５記載の記録装置。

７．前記保護情報保持部は、

前記保護情報のうち、前記暗号化コンテンツデータごとのアクセスの制限に対する第２の保守情報を保持する第２の保守情報保持部を含み、

前記制御部は、前記第２の保守情報に応じて、前記第１の記憶部に保持され、前記第２の保守情報に対応する暗号化コンテンツデータの消去を禁止する、請求項１記載の記録装置。

８．前記制御部は、外部から前記暗号化コンテンツデータの再生動作が指示された場合、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項６記載の記録装置。

９．前記制御部は、外部から与えられるユーザ情報と前記第１のユーザ特定データとが一致する場合に、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項８記載の記録装置。

１０．前記制御部は、前記ユーザ情報保持部に前記第１のユーザ特定データが未登録の場合に、前記第１の記憶部を制御して、前記第２の保守情報に応じて、前記第１の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項８記載の記録装置。

１１．（補正後）前記制御部は、外部から与えられるユーザ情報と前記第１のユーザ特定データとが一致する場合に、前記第１および第２の保守情報のうち、少なくとも１つの保守情報を書きかえることを許可する、請求項６記載の記録装置。

１２．（補正後）前記制御部は、前記ユーザ情報保持部に前記第１のユーザ特定

データが未登録の場合に、前記第１および第２の保守情報のうち、少なくとも１つの保守情報を書きかえることを許可する、請求項６記載の記録装置。

１３．前記記録装置は、

前記暗号化コンテンツデータにそれぞれ対応し、前記暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第２の記憶部（１５００）をさらに備え、

前記制御部は、外部から前記第１の記憶部に保持された前記暗号化コンテンツデータの移動が指示された場合、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データとの比較結果に応じて、前記第２の記憶部を制御して、前記ライセンス情報データを前記データ入出力部に与える、請求項１記載の記録装置。

１４．前記記録装置は、

前記暗号化コンテンツデータにそれぞれ対応し、前記暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第２の記憶部をさらに備え、

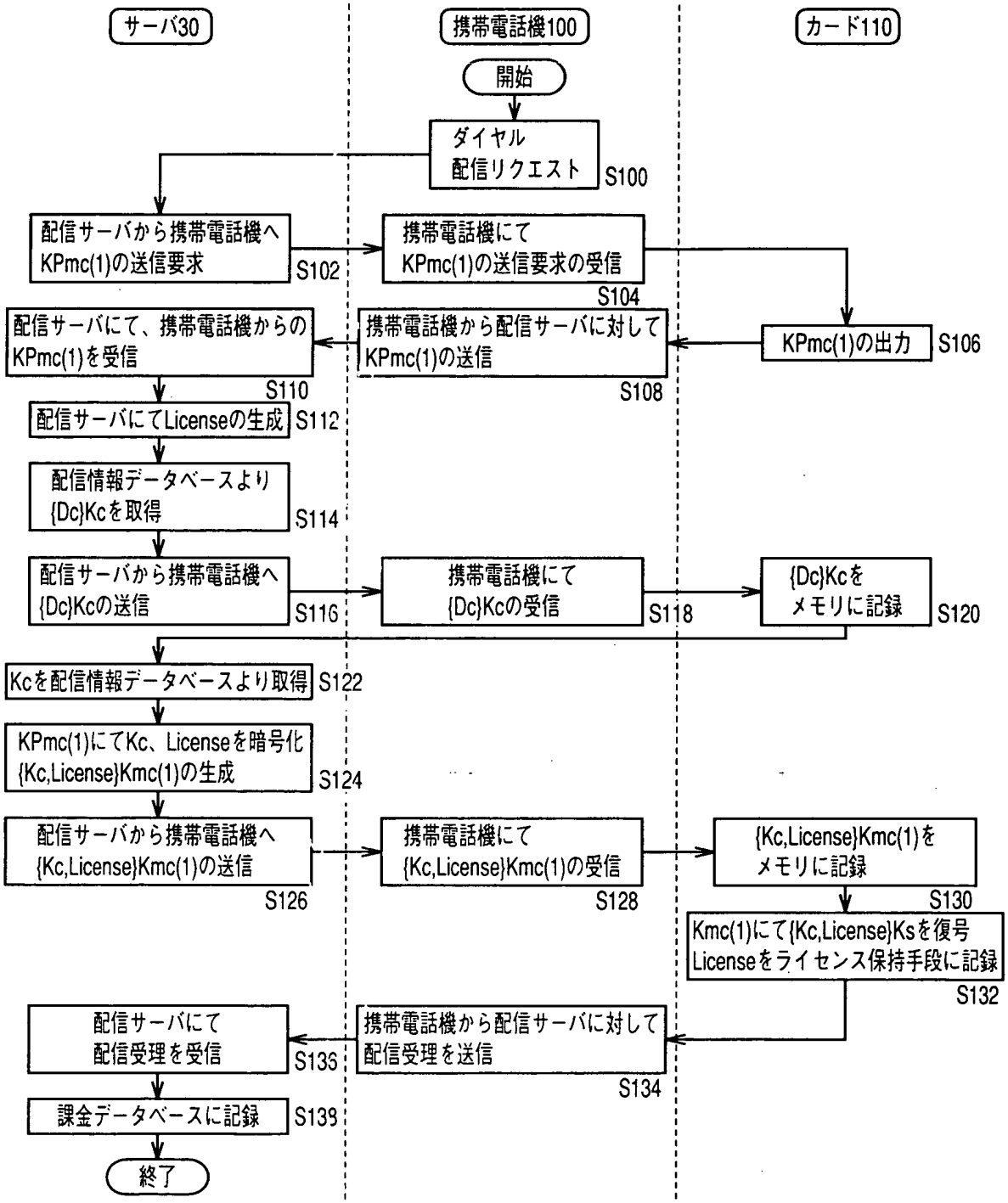
前記ライセンス情報の各々は、前記暗号化コンテンツデータごとに対応するコンテンツユーザ特定データを含み、

前記制御部は、外部から前記第１の記憶部に保持された前記暗号化コンテンツデータの移動が指示された場合、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データと、前記コンテンツユーザ特定データとの比較結果に応じて、前記第２の記憶部を制御して、前記暗号化コンテンツデータごとに前記ライセンス情報データを前記データ入出力部に与える、請求項１記載の記録装置。

１５．前記制御部は、外部から与えられる前記再生装置に対する第２のユーザ特定データと、前記ユーザ情報保持部に保持される前記第１のユーザ特定データとの比較結果に応じて、前記コンテンツユーザ特定データの変更を許可する、請求項１４記載の記録装置。

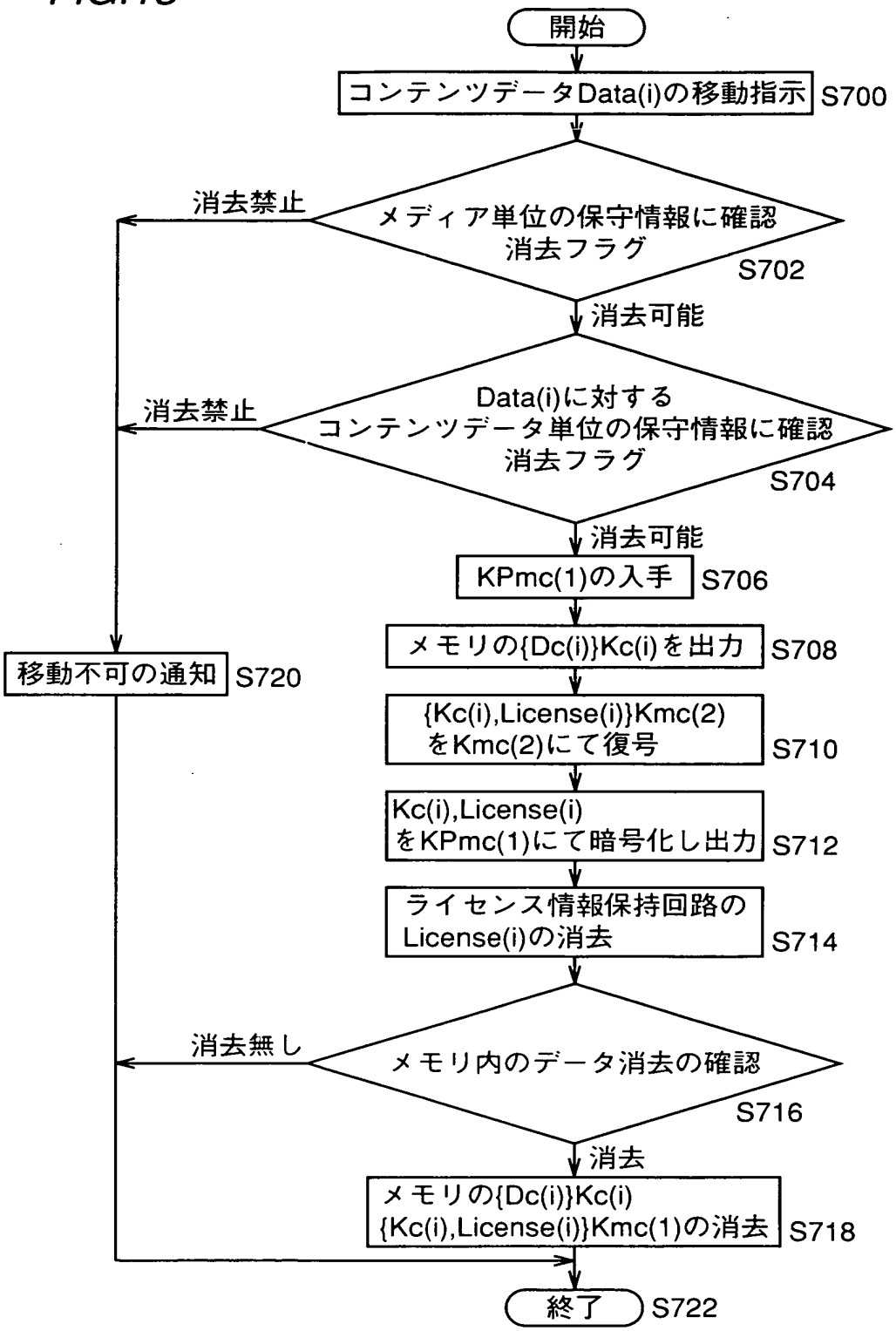
１６．前記コンテンツユーザ特定データは、対応する前記暗号化コンテンツデータの配信の際に前記ユーザ情報保持部に保持される前記第１のユーザ特定データ

FIG.6



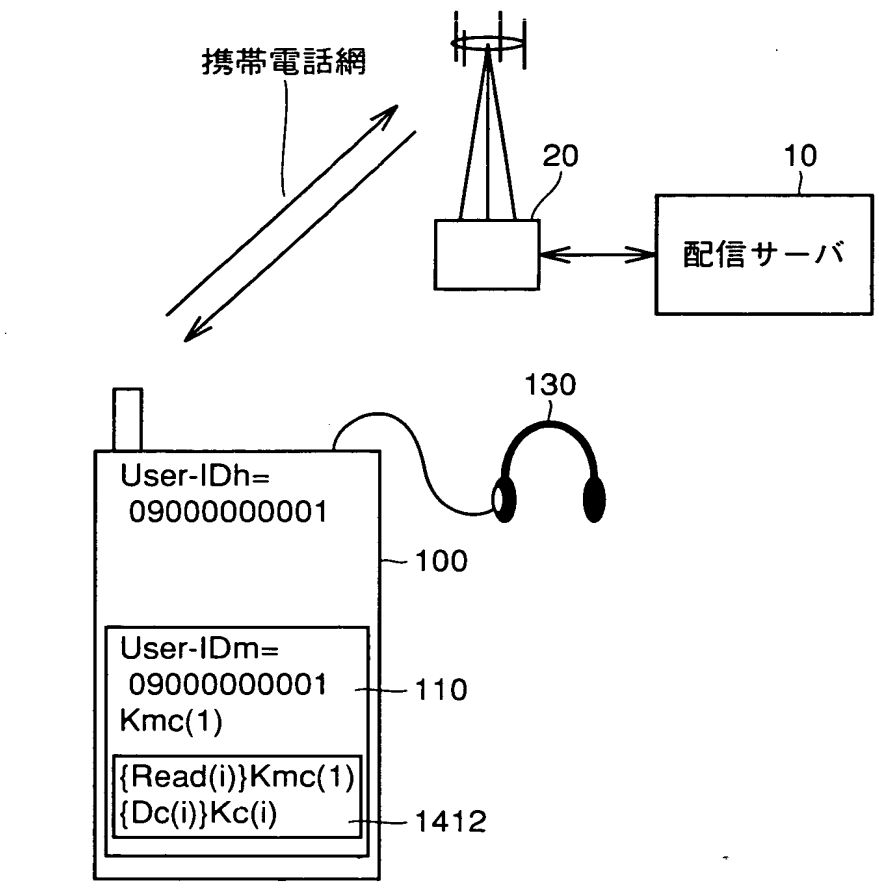
補正された用紙(条約第34条)

FIG.13



補正された用紙(条約第34条)

FIG.15



補正された用紙(条約第34条)

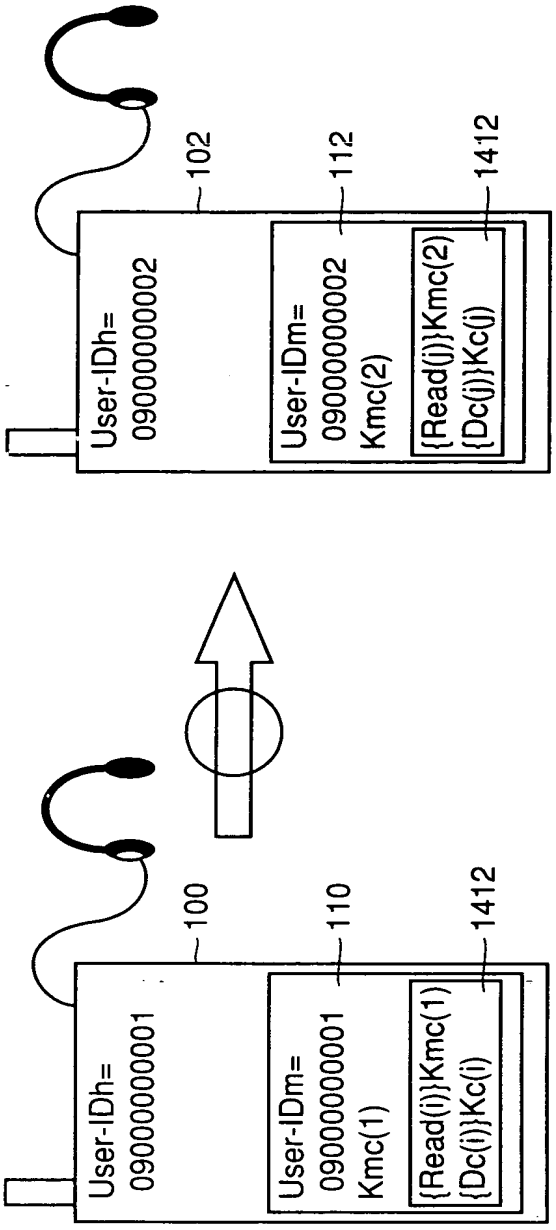


FIG.16

補正された用紙(条約第34条)

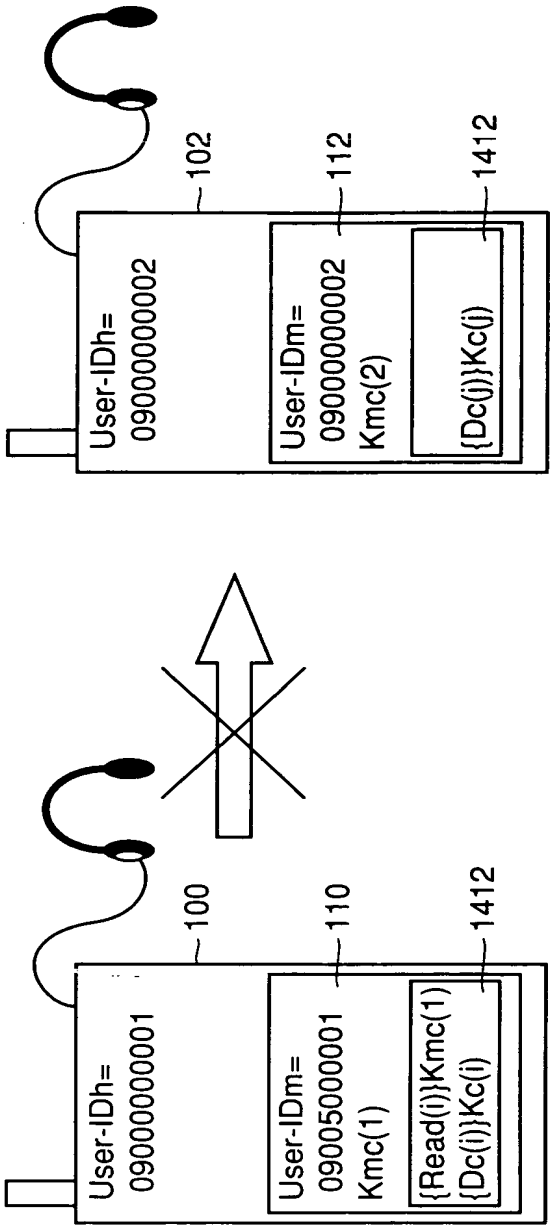
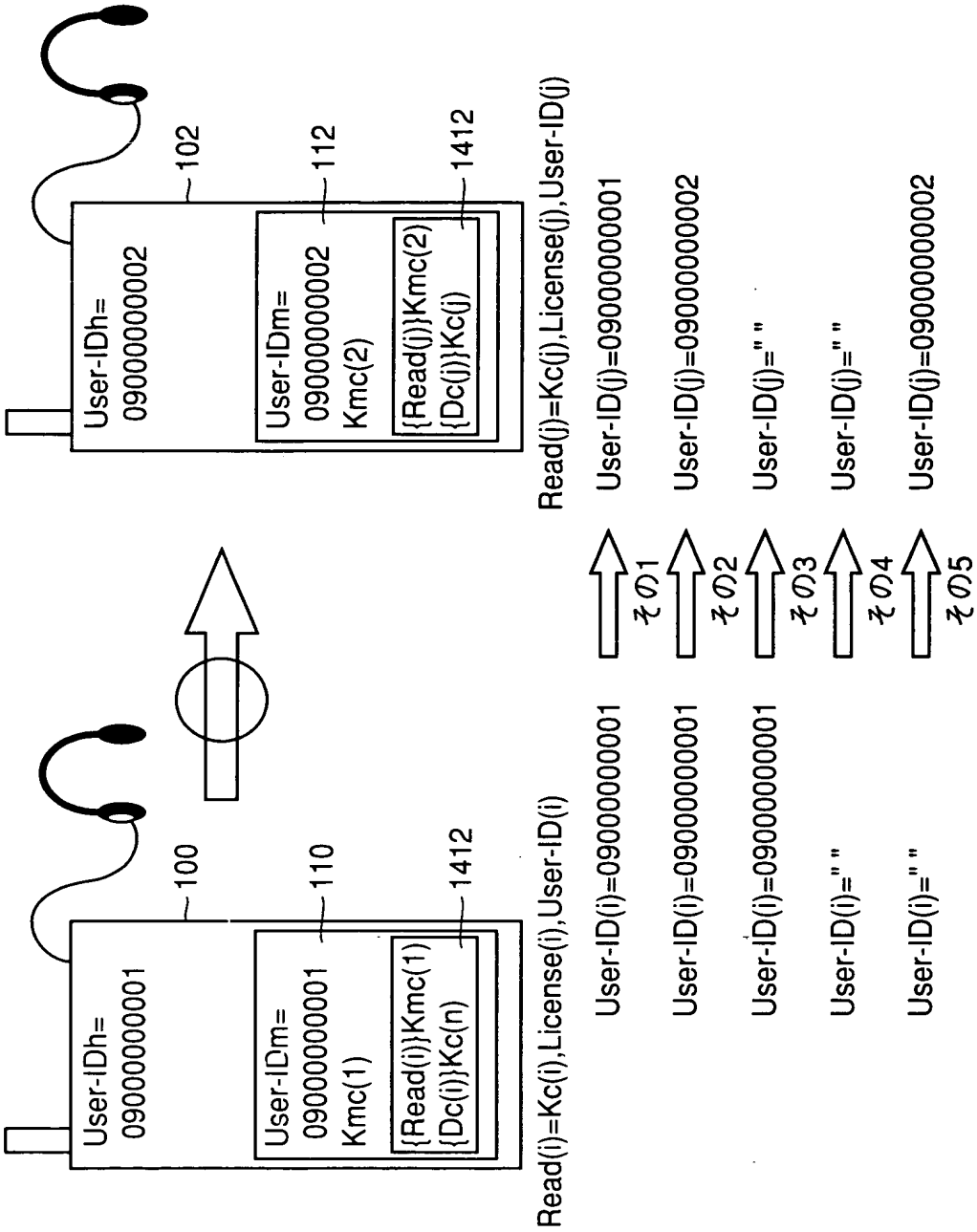


FIG.17

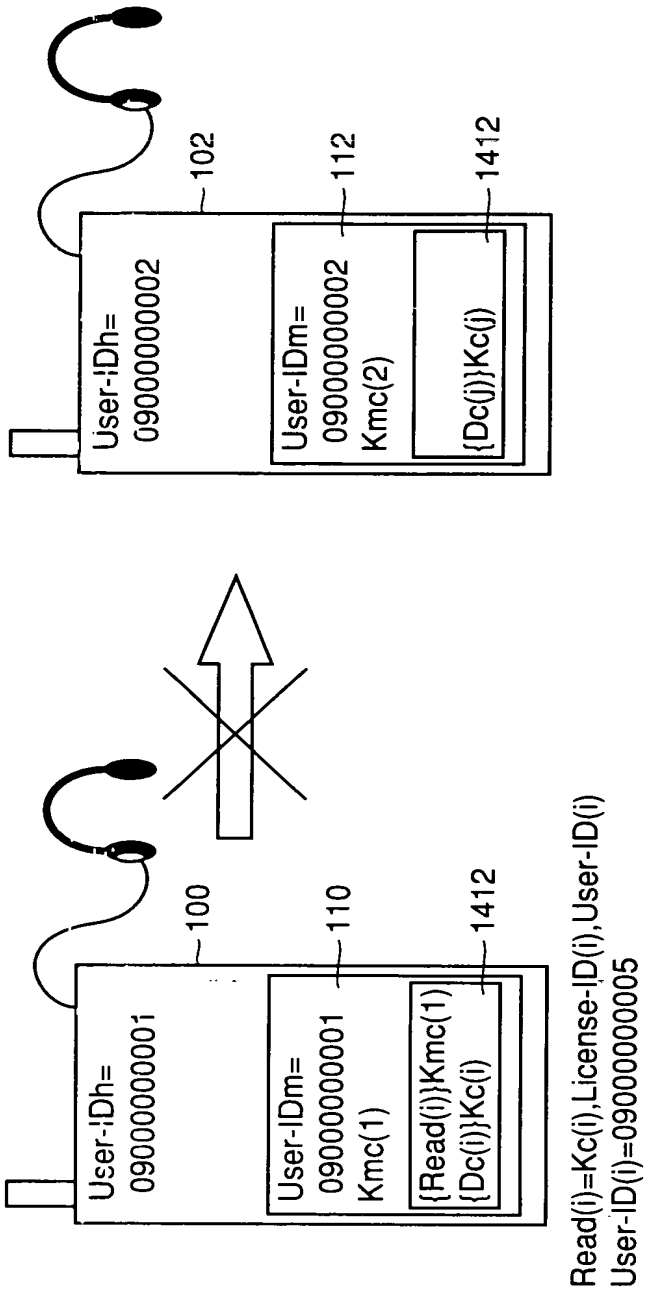
補正された用紙(条約第34条)

FIG.18



補正された用紙(条約第34条)

FIG.19



補正された用紙(条約第34条)